คู่มือปฏิบัติงาน
การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร

วงเวียน วงค์กะโซ่
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
สำนักส่งเสริมวิชาการและงานทะเบียน
มหาวิทยาลัยราชภัฏสกลนคร

คำนำ

คู่มือการปฏิบัติงานเรื่อง **“การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย”** นี้ จัดทำขึ้นโดยสำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร มีวัตถุประสงค์เพื่อใช้เป็นแนวทางในการปฏิบัติงานของบุคลากรที่เกี่ยวข้อง ตลอดจนเสริมสร้างความเข้าใจในขั้นตอนกระบวนการ และแนวทางที่ถูกต้องในการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย เพื่อให้สามารถให้บริการระบบสารสนเทศของหน่วยงานได้อย่างมีประสิทธิภาพและต่อเนื่อง

เนื้อหาในคู่มือนี้ได้ระบุถึงขั้นตอนการดำเนินงาน วิธีการปฏิบัติงาน ตลอดจนบทบาทและหน้าที่ความรับผิดชอบของผู้ปฏิบัติงานในแต่ละขั้นตอนอย่างชัดเจน เพื่อให้การปฏิบัติงานเป็นไปในทิศทางเดียวกัน มีมาตรฐาน และสามารถใช้ทรัพยากรที่มีอยู่ได้อย่างเกิดประโยชน์สูงสุด

ผู้จัดทำหวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้จะเป็นประโยชน์แก่บุคลากรผู้ปฏิบัติงานและสามารถนำไปใช้เป็นแนวทางในการปฏิบัติงานได้อย่างถูกต้อง มีคุณภาพ และสอดคล้องกับพันกิจของหน่วยงานตามที่ได้ตั้งเป้าหมายไว้

วงเวียน วงค์กะโซ่

สารบัญ

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญ

สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร เป็นหน่วยงานที่ให้บริการวิชาการแก่อาจารย์ นักศึกษา และผู้ใช้บริการโดยยึดหลักความถูกต้องและรวดเร็วตามระเบียบและข้อบังคับ โดยมีการแบ่งโครงสร้างของหน่วยงาน ออกเป็น 4 งาน ได้แก่ งานบริหารทั่วไป งานรับเข้านักศึกษา งานบริการการศึกษา และงานส่งเสริมวิชาการ ซึ่งในส่วนของงานบริการการศึกษา ดำเนินการเกี่ยวกับงานประมวลผลการเรียน หลักสูตรและแผนการเรียน จัดตารางเรียนตารางสอน งานพัฒนาระบบสารสนเทศ ปฏิบัติงานร่วมกันหรือสนับสนุนปฏิบัติงานของหน่วยงานอื่นๆ ที่เกี่ยวข้องหรือได้รับมอบหมาย โดยเฉพาะการนำเทคโนโลยีคอมพิวเตอร์ มาช่วยในการเพิ่มประสิทธิภาพการให้บริการภายในหน่วยงาน และนักศึกษาในรูปแบบออนไลน์ สอดคล้องกับภารกิจของหน่วยงาน ที่เน้นการใช้เทคโนโลยีเพื่อให้บริการ บนพื้นฐานความถูกต้อง

อย่างไรก็ตามในการปฏิบัติงานของเจ้าหน้าที่ประจำฝ่ายที่รับผิดชอบ ในส่วนของการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน นั้นย่อมมีปัญหาและอุปสรรคในการปฏิบัติงานของผู้ปฏิบัติและยังขาดการรวบรวมขั้นตอนการปฏิบัติงานที่ชัดเจน ซึ่งส่งผลให้เจ้าหน้าที่ประจำฝ่ายงานที่ได้รับมอบหมายไม่สามารถปฏิบัติงานแทนกันได้ เกิดความผิดพลาดและความล่าช้าในการปฏิบัติงาน ดังนั้นเพื่อให้เจ้าหน้าที่ประจำฝ่ายงานสามารถปฏิบัติงานแทนกันได้และลดข้อผิดพลาดในการปฏิบัติงานสามารถปฏิบัติงานเป็นมาตรฐานเดียวกัน จำเป็นต้องมีคู่มือการปฏิบัติงานที่รวบรวมขั้นตอนการปฏิบัติงานในแต่ละขั้นตอนการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน เพื่อเป็นแนวทางในการปฏิบัติงานให้เป็นไปตามขั้นตอนและมีมาตรฐานในการปฏิบัติงานให้เป็นไปในรูปแบบเดียวกัน สามารถแก้ไขปัญหาต่างๆ ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ มีความถูกต้องของข้อมูลและรวดเร็วในการปฏิบัติงานของผู้ที่มีหน้าที่รับผิดชอบ

จากความเป็นมาและความสำคัญดังกล่าว ผู้เขียนจึงมีความสนใจเขียนคู่มือการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย เพื่อใช้ภายในสำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร

วัตถุประสงค์

1. เพื่อเป็นแนวทางในการปฏิบัติการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร

2. เพื่อให้การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร เป็นมาตรฐานเดียวกัน

ประโยชน์ที่คาดว่าจะได้รับ

1. นักวิชาการคอมพิวเตอร์ใช้เป็นแนวทางการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร

2. การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร เป็นมาตรฐานเดียวกัน

ขอบเขตของคู่มือ

คู่มือการปฏิบัติงาน เรื่อง การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนครนี้ครอบคลุมวิธีการดำเนินงานติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่ายทุกขั้นตอนตามหลักวิธีการปฏิบัติในการติดตั้งระบบปฏิบัติการที่เป็นสากลภายใต้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร พ.ศ. 2557 ตามแนวปฏิบัติการจัดทำระบบสำรองและแผนการเตรียมความพร้อมกรณีฉุกเฉินหรือไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถกู้ระบบคืนกลับมาได้ภายในระยะเวลาที่เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของมหาวิทยาลัย

คำจำกัดความเบื้องต้น

การจัดทำคู่มือการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร ฉบับนี้มีการนิยามศัพท์เฉพาะและให้คำจำกัดความ ดังนี้

มหาวิทยาลัย หมายถึง มหาวิทยาลัยราชภัฏสกลนคร

สำนักงาน หมายถึง สำนักส่งเสริมวิชาการและงานทะเบียน

งานบริหารงานทั่วไป หมายถึง กลุ่มงานธุรการและงานสารบรรณ มีหน้าที่รับผิดชอบเกี่ยวกับงานธุรการและงานสารบัญ ดำเนินการประกันคุณภาพภายใน ดำเนินการตอบสนองการประเมินผลการปฏิบัติราชการ ตามคำรับรองการปฏิบัติราชการของส่วนราชการ ปฏิบัติงานร่วมกันหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นๆ ที่เกี่ยวข้องหรือได้รับมอบหมาย

งานทะเบียนและรับเข้านักศึกษา หมายถึง ดำเนินการเกี่ยวกับงานทะเบียนประมวลผล และสถิตินักศึกษา และงานระบบฐานข้อมูล งานแนะแนวประชาสัมพันธ์ ปฏิบัติงานร่วมกันหรือสนับสนุนปฏิบัติงานของหน่วยงานอื่นๆ ที่เกี่ยวข้องหรือได้รับมอบหมาย

งานบริการการศึกษาและสารสนเทศ หมายถึง ดำเนินการเกี่ยวกับงานประมวลผลการเรียน หลักสูตรและแผนการเรียน จัดตารางเรียนตารางสอน งานพัฒนาระบบสารสนเทศ ปฏิบัติงานร่วมกันหรือสนับสนุนปฏิบัติงานของหน่วยงานอื่นๆ ที่เกี่ยวข้องหรือได้รับมอบหมาย

งานส่งเสริมและพัฒนาวิชาการ หมายถึง ส่งเสริมและประสานงานพัฒนางานวิชาการผลงานทางวิชาการของอาจารย์ในมหาวิทยาลัย ส่งเสริมและพัฒนาคณาจารย์ กลั่นกรองและพิจารณาเอกสารหลักฐานที่เกี่ยวข้อง ประสานงานผู้ทรงคุณวุฒิพิจารณาตำแหน่งทางวิชาการ จัดประชุมคณะอนุกรรมการประเมินผลการสอนและคุณภาพทางวิชาการเพื่อขอกำหนด ปฏิบัติงานร่วมกันหรือสนับสนุนปฏิบัติงานของหน่วยงานอื่นๆ ที่เกี่ยวข้องหรือได้รับมอบหมาย

งานหลักสูตรและมาตรฐานการศึกษา หมายถึง สนับสนุนการพัฒนาหลักสูตร และการจัดการเรียนการสอนแก่หน่วยงานต่างๆของมหาวิทยาลัย ประกันคุณภาพการศึกษาการบริหารจัดการหลักสูตรระดับมหาวิทยาลัยร่วมกับบัณฑิตและงานประกันคุณภาพการศึกษามหาวิทยาลัย ปฏิบัติงานร่วมกันหรือสนับสนุนปฏิบัติงานของหน่วยงานอื่นๆ ที่เกี่ยวข้องหรือได้รับมอบหมาย

เจ้าหน้าที่ประจำฝ่ายงาน หมายถึง เจ้าหน้าที่ผู้ปฏิบัติงานสำนักส่งเสริมวิชาการและงานทะเบียน ฝ่ายเทคนิคคอมพิวเตอร์

เครื่องคอมพิวเตอร์แม่ข่าย หมายถึง เซิร์ฟเวอร์ (Server) หรือ เครื่องบริการ หรือเครื่องแม่ข่าย คือ เครื่องหรือโปรแกรมคอมพิวเตอร์ซึ่งทางานให้บริการ ในระบบเครือข่ายแก่ลูกข่าย (ซึ่งให้บริการผู้ใช้อีกทีหนึ่ง) เครื่องคอมพิวเตอร์ที่ทาหน้าที่เป็นเซิร์ฟเวอร์นี้ควรจะมีประสิทธิภาพสูง มีความเสถียร สามารถให้บริการแก่ผู้ใช้ได้เป็นจานวนมาก ภายในเซิร์ฟเวอร์ให้บริการได้ด้วยโปรแกรมบริการ ซึ่งทางานอยู่บนระบบปฏิบัติการอีกชั้นหนึ่ง

เครื่องคอมพิวเตอร์ลูกข่าย หรือ ไคลเอนต์ (Client) หมายถึง ระบบหรือแอปพลิเคชันที่สามารถเชื่อมต่อเข้ากับระบบคอมพิวเตอร์อื่นที่เรียกว่าเซิร์ฟเวอร์ได้ คำว่าไคลเอนต์เริ่มมีการใช้เรียกถึงคอมพิวเตอร์ที่ไม่สามารถเรียกใช้งานโปรแกรมคอมพิวเตอร์ในตัวเองได้ แต่สามารถใช้งานโปรแกรมนั้นผ่านทางระบบเครือข่าย

ระบบปฏิบัติการ (Operating System) เป็นซอฟต์แวร์พื้นฐานที่ทำหน้าที่ควบคุมและจัดการทรัพยากรต่าง ๆ บนคอมพิวเตอร์ เช่น ฮาร์ดแวร์ (Hardware), ซอฟต์แวร์ (Software), และอุปกรณ์ต่อพ่วงอื่น ๆ เพื่อให้การทำงานเกิดขึ้นได้อย่างเป็นระบบและเป็นประสบการณ์ที่สมบูรณ์

ระบบปฏิบัติการมีหน้าที่สำคัญอย่างมาก ได้แก่:

- การจัดการทรัพยากร: ระบบปฏิบัติการควบคุมและจัดการทรัพยากรต่าง ๆ บนเครื่องคอมพิวเตอร์ เช่น CPU, RAM, ฮาร์ดไดรฟ์, และอุปกรณ์อื่น ๆ เพื่อให้ทรัพยากรเหล่านี้ถูกใช้งานอย่างมีประสิทธิภาพและเป็นระบบ
- การสื่อสารระหว่างซอฟต์แวร์และฮาร์ดแวร์: ระบบปฏิบัติการทำหน้าที่เป็นตัวกลางในการสื่อสารระหว่างซอฟต์แวร์และฮาร์ดแวร์ โดยให้ซอฟต์แวร์เข้าถึงและใช้งานฮาร์ดแวร์ได้อย่างถูกต้องและปลอดภัย
- การจัดการกับการทำงานของโปรแกรม: ระบบปฏิบัติการคอยจัดการกับการทำงานของโปรแกรมที่ทำงานบนเครื่องคอมพิวเตอร์ รวมถึงการจัดการกับการทำงานพร้อมกันของหลายๆ โปรแกรมพร้อมกัน
- การให้บริการแก่ผู้ใช้: ระบบปฏิบัติการมุ่งเน้นในการให้บริการแก่ผู้ใช้ โดยทำให้ผู้ใช้สามารถเข้าถึงและใช้งานเครื่องคอมพิวเตอร์ได้อย่างสะดวกสบายและปลอดภัย

ระบบปฏิบัติการมีหลายรูปแบบและเวอร์ชั่นต่าง ๆ ซึ่งมีความแตกต่างกันตามวัตถุประสงค์และการใช้งาน เช่น Windows, macOS, Linux เป็นต้น แต่ทุกแบรนด์ก็มีความสำคัญในการควบคุมและจัดการทรัพยากรของเครื่องคอมพิวเตอร์ในลักษณะที่แตกต่างกันไป ตามความเหมาะสมของผู้ใช้งานและการใช้งานที่ต้องการ

ระบบเครือข่าย หมายถึง ระบบที่มีการนำคอมพิวเตอร์อย่างน้อยสองเครื่องมาเชื่อมต่อกัน โดยใช้สื่อกลาง เพื่อใช้ในการสื่อสารข้อมูลถึงกันได้อย่างมีประสิทธิภาพ ซึ่งทำให้ผู้ใช้คอมพิวเตอร์แต่ละเครื่องสามารถใช้แลกเปลี่ยนข้อมูลซึ่งกันและกันได้ นอกจากนี้ยังสามารถใช้ทรัพยากรร่วมกัน ทำให้ประหยัดทรัพยากรในการใช้งาน

เครือข่ายคอมพิวเตอร์หรือคอมพิวเตอร์เน็ตเวิร์ค (Computer Network) เป็นการเชื่อมต่อคอมพิวเตอร์และอุปกรณ์ต่าง ๆ เข้าด้วยกันเพื่อสื่อสารแลกเปลี่ยนข้อมูลระหว่างกันผ่านสื่อต่าง ๆ เช่น สายสัญญาณ, สายแบบไร้สาย, และเครือข่ายอินเตอร์เน็ต (Internet) เพื่อให้สามารถแบ่งปันข้อมูล, ทรัพยากร, และบริการต่าง ๆ ระหว่างผู้ใช้งานได้อย่างมีประสิทธิภาพและปลอดภัย

การเชื่อมต่อเครือข่ายคอมพิวเตอร์สามารถทำได้ในหลายลักษณะ เช่น:

- เครือข่ายแบบมีสาย (Wired Network): การเชื่อมต่อโดยใช้สายสัญญาณเช่น เคเบิลเอเธอร์เน็ต (Ethernet cable) หรือสายไฟเบอร์ออปติค (Fiber optic cable) เพื่อส่งข้อมูลระหว่างอุปกรณ์
- เครือข่ายแบบไร้สาย (Wireless Network): การเชื่อมต่อโดยใช้สัญญาณไร้สาย เช่น Wi-Fi ที่ช่วยให้อุปกรณ์สามารถเชื่อมต่อกับเครือข่ายได้โดยไม่ต้องใช้สายสัญญาณ
- เครือข่ายแบบเข้ารหัส (Encrypted Network): เครือข่ายที่มีการเข้ารหัสข้อมูลเพื่อความปลอดภัย เช่น เครือข่าย Wi-Fi ที่ใช้รหัสผ่าน (password) เพื่อรับสัญญาณและเข้าถึงเครือข่าย
- เครือข่ายอินเตอร์เน็ต (Internet Network): เครือข่ายที่เชื่อมต่อกับโลกอินเตอร์เน็ต ซึ่งเป็นเครือข่ายที่ใหญ่ที่สุดและมีการเชื่อมต่อทั่วโลกผ่านอินเทอร์เน็ต

เครือข่ายคอมพิวเตอร์มีบทบาทสำคัญในการให้บริการต่าง ๆ เช่น การแชร์ไฟล์ การเข้าถึงข้อมูล การสื่อสารผ่านอีเมล การใช้บริการอินเทอร์เน็ต, และการเชื่อมต่อเครื่องพิมพ์หรืออุปกรณ์อื่นๆ ที่เชื่อมต่อในเครือข่ายได้

เว็บเซิร์ฟเวอร์ (Web Server) คือ โปรแกรมคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการจัดการและนำเสนอเนื้อหาหน้าเว็บ (Web content) ต่าง ๆ ให้แก่ผู้ใช้งานผ่านทางโปรโตคอล HTTP (Hypertext Transfer Protocol) หรือ HTTPS (HTTP Secure) ซึ่งเป็นโปรโตคอลสำหรับการสื่อสารข้อมูลผ่านเครือข่ายอินเทอร์เน็ต (Internet) โดยทั่วไปแล้ว เว็บเซิร์ฟเวอร์มักจะใช้ซอฟต์แวร์เซิร์ฟเวอร์เช่น Apache HTTP Server, Nginx, Microsoft IIS (Internet Information Services), หรือซอฟต์แวร์เซิร์ฟเวอร์อื่น ๆ ในการให้บริการเนื้อหาหน้าเว็บแก่ผู้ใช้งาน โดยส่วนมากจะใช้งานบนเครื่องเซิร์ฟเวอร์ที่มีการเชื่อมต่อกับอินเทอร์เน็ต และมีการติดตั้งซอฟต์แวร์เซิร์ฟเวอร์พร้อมกับเนื้อหาของเว็บไซต์ในระบบปฏิบัติการ เช่น Windows, Linux, Unix เป็นต้น ผู้ใช้งานสามารถเข้าถึงเว็บเซิร์ฟเวอร์ผ่านทางเว็บเบราว์เซอร์ เพื่อร้องขอข้อมูลหรือบริการต่าง ๆ ที่เว็บเซิร์ฟเวอร์ได้เตรียมไว้ เช่น หน้า HTML, ภาพ, ไฟล์เสียง, วิดีโอ, และแอปพลิเคชันเว็บต่าง ๆ ซึ่งจะถูกส่งกลับมายังผู้ใช้งานผ่านทางโปรโตคอล HTTP/HTTPS ตามคำขอที่ได้รับ

เว็บไซต์ (Website) หมายถึง ชุดข้อมูลที่ถูกจัดเรียงและแสดงผลในรูปแบบของหน้าเว็บบนอินเทอร์เน็ต เป็นการนำเสนอข้อมูลหรือเนื้อหาต่าง ๆ ในรูปแบบของหน้าเว็บที่สามารถเข้าถึงได้ผ่านทางเว็บเบราว์เซอร์ ซึ่งเนื้อหาบนเว็บไซต์อาจประกอบด้วยข้อความ เรื่องราว เสียง ภาพ วิดีโอ และฟีเจอร์ต่าง ๆ ตามวัตถุประสงค์ของเว็บไซต์นั้น ๆ

เว็บไซต์มักจะประกอบด้วยหลายหน้าเว็บ (web pages) ที่เชื่อมโยงกัน โดยมักจะมีหน้าหลัก (homepage) เป็นจุดเริ่มต้นที่เข้าสู่เว็บไซต์ และมีหน้าย่อย (sub-pages) หรือเนื้อหาเพิ่มเติมอื่น ๆ ที่ผู้ใช้งานสามารถนำเสนอข้อมูลหรือบริการต่าง ๆ ได้ เช่น เว็บไซต์ข่าว บล็อก ร้านค้าออนไลน์ เว็บไซต์ข้อมูลขององค์กรหรือบริษัท แอปพลิเคชันเว็บ เป็นต้น คำว่า "เว็บไซต์" สามารถเขียนแบบย่อได้เป็น "เว็บ" หรือ "เว็บไซต์" โดยมักใช้ในที่และเวลาที่เหมาะสมตามบริบทที่ใช้งาน

โพรโทคอล (protocol) คือ ชุดกฎหรือข้อกำหนด ที่กำหนดวิธีการสื่อสารระหว่างอุปกรณ์หรือระบบต่างๆ เปรียบเสมือนภาษาที่ใช้ในการติดต่อสื่อสาร ทำให้อุปกรณ์ต่างๆ เข้าใจกันและทำงานร่วมกันได้ โพรโทคอลมีหลากหลายประเภท ขึ้นอยู่กับวัตถุประสงค์การใช้งาน

ตัวอย่างโพรโทคอลที่ใช้กันทั่วไป

- HTTP (Hyper Text Transfer Protocol): ใช้สำหรับการรับส่งข้อมูลบนเว็บ เช่น การโหลดหน้าเว็บ ดาวน์โหลดไฟล์
- TCP/IP (Transmission Control Protocol/Internet Protocol): ใช้สำหรับการเชื่อมต่อและรับส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต
- SMTP (Simple Mail Transfer Protocol): ใช้สำหรับการส่งอีเมล
- FTP (File Transfer Protocol): ใช้สำหรับการถ่ายโอนไฟล์
- SSH (Secure Shell): ใช้สำหรับการเข้าถึงระบบระยะไกลอย่างปลอดภัย

ประโยชน์ของโพรโทคอล:

- ทำให้การสื่อสารมีประสิทธิภาพ: โพรโทคอลกำหนดวิธีการสื่อสารที่ชัดเจน ทำให้อุปกรณ์ต่างๆ เข้าใจกันและทำงานร่วมกันได้อย่างราบรื่น
- เพิ่มความน่าเชื่อถือ: โพรโทคอลมีกลไกตรวจสอบความผิดพลาดและแก้ไข ทำให้การสื่อสารมีความน่าเชื่อถือ
- เพิ่มความปลอดภัย: โพรโทคอลบางชนิดมีกลไกการเข้ารหัสข้อมูล ทำให้การสื่อสารมีความปลอดภัย

สรุป โพรโทคอลเป็นองค์ประกอบสำคัญในการสื่อสารของอุปกรณ์และระบบต่างๆ เปรียบเสมือนภาษาที่ใช้ในการติดต่อสื่อสาร ทำให้อุปกรณ์ต่างๆ เข้าใจกันและทำงานร่วมกันได้ โพรโทคอลมีหลากหลายประเภท ขึ้นอยู่กับวัตถุประสงค์การใช้งาน

เกตเวย์ (Gateway) หมายถึง อุปกรณ์ที่ทำหน้าที่เชื่อมต่อระหว่างเครือข่ายคอมพิวเตอร์หรือระบบเครือข่ายที่แตกต่างกัน เพื่อให้การสื่อสารและการส่งข้อมูลระหว่างเครือข่ายเหล่านั้นสามารถทำได้ โดยเกตเวย์สามารถแปลงข้อมูลหรือโปรโตคอลที่ใช้ในระบบเครือข่ายหนึ่งเป็นรูปแบบที่เหมาะสมสำหรับเครือข่ายอีกต่างหาก

อินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายคอมพิวเตอร์ขนาดใหญ่ ที่เกิดจากการเชื่อมต่อกันของเครือข่ายคอมพิวเตอร์ขนาดเล็กและขนาดใหญ่มากมายทั่วโลก ผู้ใช้สามารถเข้าถึงข้อมูลและบริการต่างๆ บนอินเทอร์เน็ตผ่านอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ สมาร์ทโฟน แท็บเล็ต ผ่านสายสื่อสารทั้งแบบมีสายและแบบไร้สาย

เว็บเบราว์เซอร์ (web browser) คือ โปรแกรมคอมพิวเตอร์ ที่ใช้ในการเข้าถึงและแสดงผล เว็บไซต์ บน อินเทอร์เน็ต เปรียบเสมือนหน้าต่างที่ช่วยให้ผู้ใช้สามารถดูข้อมูลต่างๆ บนเว็บไซต์ได้ โดยเว็บเบราว์เซอร์จะทำหน้าที่แปลง ภาษา HTML (Hypertext Markup Language) ที่ใช้สร้างเว็บไซต์ ให้เป็นหน้าเว็บที่ผู้ใช้สามารถอ่านและเข้าใจได้

Virtual Machine (VM) หรือ แมชชีนเสมือน หมายถึง ซอฟต์แวร์ที่จำลองระบบคอมพิวเตอร์แบบสมบูรณ์เสมือนจริง ทำงานคล้ายกับคอมพิวเตอร์จริงทุกประการ แต่มีทรัพยากรแยกจากระบบปฏิบัติการหลัก (Host OS)

VM ประกอบด้วย:

- Virtual CPU: ซีพียูเสมือน จำลองการทำงานของ CPU จริง
- Virtual Memory: หน่วยความจำเสมือน จำลองการทำงานของ RAM จริง
- Virtual Storage: พื้นที่เก็บข้อมูลเสมือน จำลองการทำงานของฮาร์ดดิสก์จริง
- Virtual Network Interface: อินเทอร์เฟซเครือข่ายเสมือน จำลองการทำงานของการ์ดเครือข่ายจริง

การใช้งาน VM:

- ทดสอบซอฟต์แวร์: ทดสอบโปรแกรมหรือระบบปฏิบัติการใหม่ โดยไม่ต้องติดตั้งบนเครื่องจริง
- พัฒนาซอฟต์แวร์: พัฒนาโปรแกรมในสภาพแวดล้อมที่แยกจากเครื่องจริง
- ใช้งานแอปพลิเคชั่นเก่า: ใช้งานโปรแกรมเก่าที่ไม่รองรับระบบปฏิบัติการปัจจุบัน
- เพิ่มประสิทธิภาพการใช้ทรัพยากร: แบ่งทรัพยากรของคอมพิวเตอร์จริงให้ VM หลายตัวใช้งาน
- สำรองข้อมูล: สำรองข้อมูลระบบปฏิบัติการและแอปพลิเคชั่นทั้งหมด

ประเภทของ VM:

- Type 1 Hypervisor: ติดตั้งบนฮาร์ดแวร์โดยตรง ทำงานใกล้ชิดกับฮาร์ดแวร์ เหมาะสำหรับการใช้งานระดับองค์กร เช่น VMware ESXi, Microsoft Hyper-V
- Type 2 Hypervisor: ติดตั้งบนระบบปฏิบัติการ ทำงานบนระบบปฏิบัติการหลัก เหมาะสำหรับการใช้งานทั่วไป เช่น VirtualBox, VMware Fusion

ข้อดีของ VM:

- ความยืดหยุ่น: สามารถสร้าง VM ได้หลายตัวตามต้องการ
- ความปลอดภัย: แยก VM แต่ละตัวออกจากกัน ป้องกันปัญหาจาก Malware
- ความสะดวก: บริหารจัดการ VM ได้ง่าย
- ประหยัดค่าใช้จ่าย: แบ่งทรัพยากรของคอมพิวเตอร์จริงให้ VM หลายตัวใช้งาน

ข้อเสียของ VM:

-ทรัพยากร: จำเป็นต้องมีทรัพยากรฮาร์ดแวร์เพียงพอ

-ความซับซ้อน: การตั้งค่าและใช้งาน VM อาจยุ่งยากสำหรับผู้ใช้ทั่วไป

สรุป Virtual Machine เป็นเครื่องมือที่มีประโยชน์สำหรับการใช้งานหลายประเภท ช่วยเพิ่มประสิทธิภาพการใช้ทรัพยากร ความปลอดภัย และความยืดหยุ่น

บทที่ 2
โครงสร้างและหน้าที่ความรับผิดชอบ

2.1 โครงสร้างหน่วยงาน

โรงเรียนฝึกหัดครูสกลนคร ก่อตั้งเมื่อวันที่ 17 กรกฎาคม 2507 ต่อมาวันที่ 16 มกราคม 2513 ได้ยกฐานะเป็นวิทยาลัยครูสกลนคร ซึ่งในขณะนั้นแผนกทะเบียนประวัติกับแผนกวัดผลแยกกันทำหน้าที่โดยแผนกทะเบียนประวัติทำหน้าที่เกี่ยวกับทะเบียนนักศึกษา การออกใบสุทธิ ประกาศนียบัตร ส่วนแผนกวัดผลทำหน้าที่เกี่ยวกับการลงทะเบียนวิชาเรียน และการประมวลผลการเรียน

ต่อมาในปี พ.ศ.2518 ได้ประกาศใช้ พระราชบัญญัติวิทยาลัยครู มีสภาการฝึกหัดครูเป็นคณะกรรมการหรือบอร์ดสูงสุดของวิทยาลัยครู มีหน้าที่อนุมัติปริญญาและอนุปริญญา

ในระยะเริ่มแรกวิทยาลัยครูสกลนครได้รวมแผนกทะเบียนประวัติและแผนกวัดผลเป็นหน่วยเดียวกันเรียกว่า “แผนกทะเบียนและวัดผล” ต่อมาได้เปลี่ยนเป็น “สำนักส่งเสริมวิชาการ” โดยมีหน่วยงานในสังกัด 5 หน่วยงานได้แก่ ฝ่ายเลขานุการ ฝ่ายหลักสูตรตารางสอน ฝ่ายทะเบียนนักศึกษา ฝ่ายวัดผล และฝ่ายบริการนักศึกษา

ปี พ.ศ.2538 วิทยาลัยครูสกลนคร เปลี่ยนเป็นสถาบันราชภัฏสกลนคร ตาม พ.ร.บ. สถาบัน ราชภัฏ สำนักส่งเสริมวิชาการ เปลี่ยนชื่อเป็น “สำนักทะเบียนและประมวลผล”

ปี พ.ศ.2542 สำนักทะเบียนและประมวลผลเปลี่ยนเป็น “สำนักส่งเสริมวิชาการ” ตามการจัดแบ่งหน่วยงานตาม พ.ร.บ.สถาบันราชภัฏซึ่งได้จัดแบ่งหน่วยงานในสำนักฯ ออกเป็น 5 ฝ่าย ได้แก่ ฝ่ายบริหารงานทั่วไป ฝ่ายประมวลผลการเรียน ฝ่ายทะเบียนนักศึกษา ฝ่ายหลักสูตรและแผนการเรียน ฝ่ายเทคนิคคอมพิวเตอร์

ปี พ.ศ.2547 ถึงปัจจุบันสำนักส่งเสริมวิชาการ เปลี่ยนเป็น “สำนักส่งเสริมวิชาการและงานทะเบียน” ตามประกาศโครงสร้างใหม่ของมหาวิทยาลัยราชภัฏ สำนักส่งเสริมวิชาการและงานทะเบียน มีจำนวน 4 งาน ประกอบด้วย งานบริหารงานทั่วไป งานรับเข้านักศึกษา งานบริการการศึกษา และงานส่งเสริมวิชาการ และปี พ.ศ. 2567 สำนักส่งเสริมวิชาการและงานทะเบียนได้ปรับโครงสร้างใหม่ จากเดิม 4 งาน เป็น 5 งาน ดังนี้

1. งานบริหารทั่วไป
2. งานทะเบียนและรับเข้านักศึกษา
3. งานบริการการศึกษาและสารสนเทศ
4. งานส่งเสริมและพัฒนาวิชาการ
5. งานหลักสูตรและมาตรฐานทางการศึกษา

ปรัชญา

บริการอย่างมีประสิทธิภาพ บนพื้นฐานความถูกต้อง

วิสัยทัศน์

ส่งเสริม สนับสนุนบริการงานวิชาการ ที่มีคุณภาพในระดับสากล

พันธกิจ

ให้บริการงานวิชาการแก่อาจารย์ นักศึกษา และผู้มาใช้บริการโดยยึดหลักความถูกต้องและรวดเร็วตามระเบียบและข้อบังคับ

อัตลักษณ์

บริการแบบมืออาชีพ เน้นการใช้เทคโนโลยี บนพื้นฐานความถูกต้อง

เอกลักษณ์

ยิ้มแย้มแจ่มใสเต็มใจให้บริการ

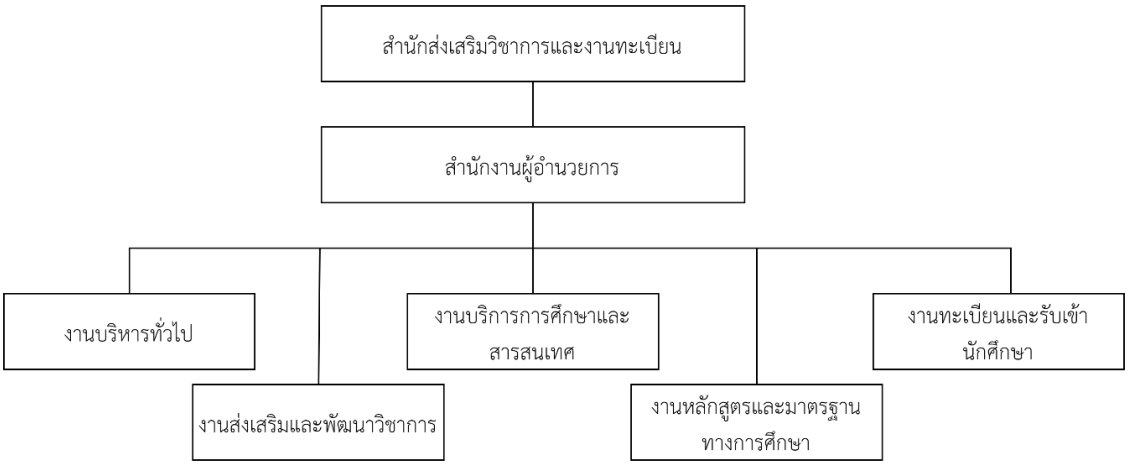
ค่านิยมหลัก

ให้การบริการที่ถูกต้อง รวดเร็วและสร้างความพึงพอใจแก่ผู้รับบริการ

2.2 โครงสร้างการบริหารจัดการ

2.2.1 โครงสร้างองค์กร (Organization chart)

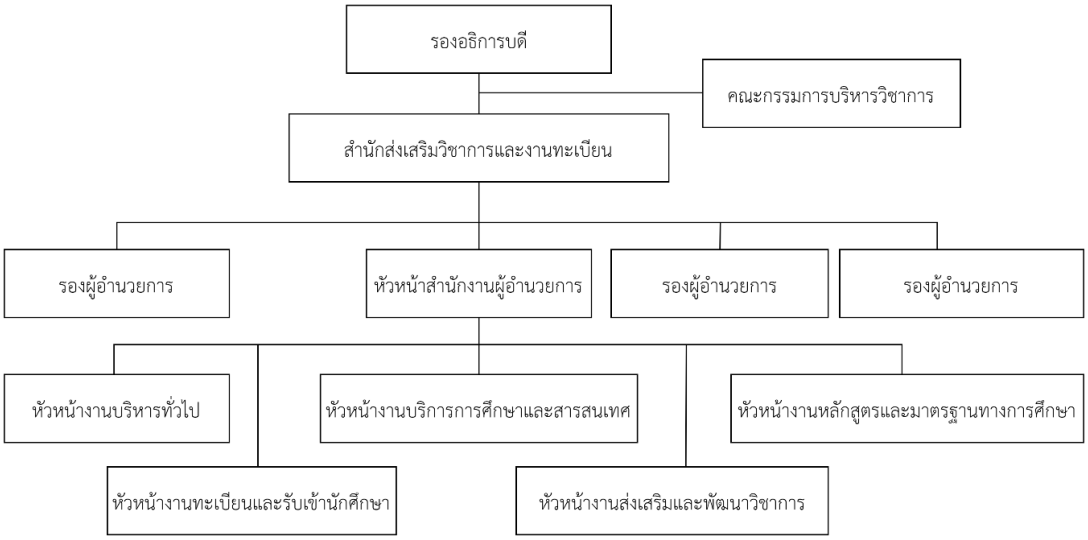
โครงสร้างการแบ่งส่วน หน่วยงานในสำนักงานผู้อำนวยการ สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร



ภาพประกอบ 1 โครงสร้างองค์กร

2.2.2 โครงสร้างการบริหาร (Administration chart)

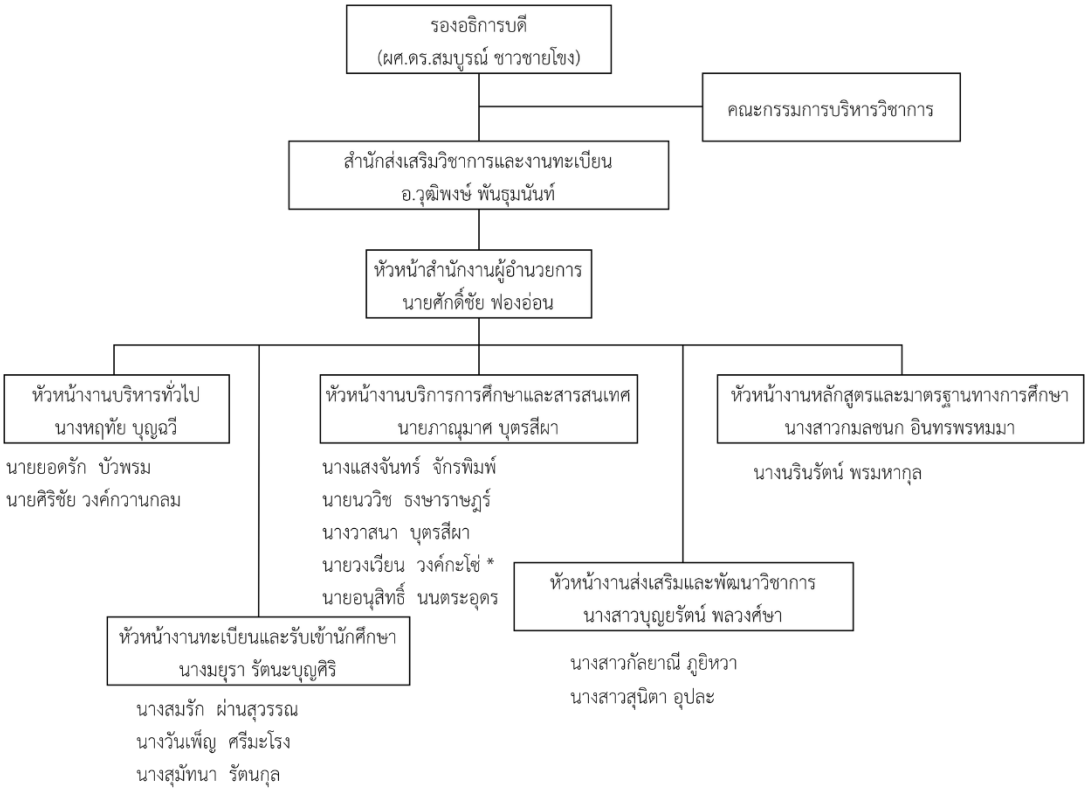
สำนักส่งเสริมวิชาการและงานทะเบียนมีโครงสร้างการบริหาร ดังนี้



ภาพประกอบ 2 โครงสร้างการบริหาร

2.2.3 โครงสร้างการปฏิบัติงาน (Activity chart)

สำนักส่งเสริมวิชาการและงานทะเบียนมีโครงสร้างการปฏิบัติงาน ดังนี้



ภาพประกอบ 3 โครงสร้างการปฏิบัติงาน

2.2.4 รายชื่อบุคลากร สำนักส่งเสริมวิชาการและงานทะเบียน

ผศ.ดร.สมบูรณ์ ชาวชายโขง
รองอธิการบดีด้านวิชาการ

นายวุฒิพงษ์ พันธุมนันท์
ผู้อำนวยการสำนักส่งเสริมวิชาการและงานทะเบียน

ผศ.ดร.นพรัตน์ สิทธิวงศ์
รองผู้อำนวยการ

ผศ.ดร.พรรณนภา หาญมนตรี
รองผู้อำนวยการ

นายเสริมวิช บุตรโยธี
รองผู้อำนวยการ

นายศักดิ์ชัย ฟองอ่อน
หัวหน้าสำนักงาน

งานบริหารทั่วไป

นางหฤทัย บุญฉวี
เจ้าหน้าที่บริหารงานทั่วไปชำนาญการ
หัวหน้างานบริหารทั่วไป

จ่าสิบตรียอดรัก บัวพรม
เจ้าหน้าที่บริหารงานทั่วไปปฏิบัติการ

นายศิริชัย วงค์กวานกลม
เจ้าหน้าที่บริหารงานทั่วไปปฏิบัติการ

งานบริการการศึกษาและสารสนเทศ

นายภาณุมาศ บุตรสีผา
นักวิชาการศึกษาชำนาญการ
หัวหน้างานบริการการศึกษาและสารสนเทศ

นางแสงจันทร์ จักรพิมพ์
นักวิชาการศึกษาปฏิบัติการ

นางวาสนา บุตรสีผา
นักวิชาการศึกษาปฏิบัติการ

นายนววิช ธงษาราษฎร์
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายวงเวียน วงค์กะโซ่*
นักวิชาการคอมพิวเตอร์ปฏิบัติการ

นายอนุสิทธิ์ นนตระอุดร
นักวิชาการศึกษาปฏิบัติการ

งานทะเบียนและรับเข้านักศึกษา

นางมยุรา รัตนบุญศิริ
นักวิชาการศึกษาปฏิบัติการ
หัวหน้างานทะเบียนและรับเข้านักศึกษา

นางวันเพ็ญ ศรีมะโรง
นักวิชาการศึกษาปฏิบัติการ

นางสุมัทนา รัตนกุล
นักวิชาการศึกษาปฏิบัติการ

นางสมรัก ผ่านสุวรรณ
พนักงานพิมพ์ดีด ส.3

งานส่งเสริมและพัฒนาวิชาการ

นางสาวบุญยรัตน์ พลวงศ์ษา
นักวิชาการศึกษาปฏิบัติการ
หัวหน้างานส่งเสริมและพัฒนาวิชาการ

นางสาวกัลยาณี ภูยิหวา
เจ้าหน้าที่บริหารงานทั่วไป

นางสาวสุนิตรา อุประ
เจ้าหน้าที่บริหารงานทั่วไป

งานหลักสูตรและมาตรฐานทางการศึกษา

นางสาวกมลชนก อินทรพรหมมา
นักวิชาการศึกษาชำนาญการ
หัวหน้างานหลักสูตรและมาตรฐานทางการศึกษา

นางสาวนรินรัตน์ พรมหากุล
นักวิชาการศึกษาปฏิบัติการ

2.3 บทบาทหน้าที่ของหน่วยงาน

งานบริหารทั่วไป หน้าที่ความรับผิดชอบ

1) การจัดทำหนังสือราชการ

2) การจัดเก็บเอกสารทางราชการ

3) การเผยแพร่เอกสารทางราชการ

4) การทำลายเอกสาร

5) การรับ – ส่งหนังสือ

6) ส่งเอกสารหน่วยงานภายนอกและภายใน

7) จัดทำประกาศกำหนดวันลงทะเบียนวิชาเรียน และกิจกรรมการเรียนการสอนของนักศึกษาภาคปกติ และภาคพิเศษ (กศ.ป.)

8) จัดทำประกาศกำหนดวันเบิกจ่ายค่าตอบแทนการสอน ค่าตอบแทนการดำเนินงานโครงการจัดการศึกษาเพื่อปวงชน (กศ.ป.)

9) จัดทำประกาศสัปดาห์หยุดมอบหมายงานของนักศึกษาภาคพิเศษ (กศ.ป.)

10) จัดทำคู่มือนักศึกษา

11) จัดดำเนินงานโครงการศึกษาดูงานของหน่วยงาน

12) ควบคุมตรวจสอบการลงเวลาปฏิบัติราชการของบุคลากรในหน่วยงาน ควบคุมการลาทุกประเภท และสรุปการลาทุกประเภทส่งผู้บริหาร

13) การเบิกจ่ายค่าสอนอาจารย์พิเศษรายชั่วโมง และค่าสอน กศ.ป.

14) การวางแผนการใช้งบประมาณ

15) การจัดทำคำขอตั้งงบประมาณประจำปี

16) การควบคุมทะเบียนครุภัณฑ์

17) การจัดซื้อจัดจ้างโดยวิธีตกลงราคา

18) การจัดซื้อวัสดุสำนักงาน

19) งานเลขานุการ

20) จัดทำคำขอจัดตั้งงบประมาณ/ขออนุมัติโครงการ

21) โครงการพัฒนาผลงานทางวิชาการของอาจารย์มหาวิทยาลัยราชภัฏสกลนคร

22) การประชุมสภาวิชาการ

23) การประชุมกรรมการบริหารวิชาการ (ก.วช.)

24) แผนงานยุทธศาสตร์

25) แผนปฏิบัติราชการ

26) แผนปฏิบัติราชการประจำปี

27) กำกับการดำเนินการจัดทำแผนพัฒนาบุคลากร

28) กำกับการดำเนินการจัดทำแผนการจัดการความรู้

29) รายงานผลตามแผนกลยุทธ์

30) รายงานผลตามแผนปฏิบัติราชการ

31) กำกับการดำเนินการจัดทำรายงานผลตามแผนพัฒนาบุคลากร

32) กำกับการดำเนินการจัดทำรายงานผลตามแผนการจัดการความรู้

33) กำกับการดำเนินการจัดทำการจัดนิทศการการจัดการความรู้

34) การใช้จ่ายงบประมาณ/การติดตามโครงการ/การประเมินผลโครงการ/การกระตุ้นการดำเนินโครงการ

35) งานประกันคุณภาพการศึกษา

36) บริหารความเสี่ยง และควบคุมภายใน

37) งานอื่น ๆ ที่ได้รับมอบหมาย

งานทะเบียนและรับเข้านักศึกษา หน้าที่รับผิดชอบ

1) จัดทำโครงการสอบคัดเลือกนักศึกษาใหม่เข้าศึกษาต่อในมหาวิทยาลัยราชภัฏสกลนคร

2) สำรวจแผนการรับนักศึกษา และลงฐานข้อมูล

3) จัดทำปฏิทินการรับนักศึกษาภาคปกติ และภาคพิเศษ (เสาร์ – อาทิตย์)

4) รับสมัครนักศึกษาใหม่ ประเภทโควตา (เรียนดี กิจกรรมดี กีฬาดี และคนดี)

5) รับสมัครนักศึกษาใหม่ ประเภทรับตรง (เฉพาะหลักสูตร ค.บ. 4 ปี)

6) รับสมัครนักศึกษาใหม่ ประเภทรับตรงทั่วไป

7) รับสมัครนักศึกษาใหม่ภาคพิเศษ (เสาร์-อาทิตย์)

8) สำรวจอาจารย์ออกข้อสอบ/อาจารย์คุมสอบ และอาจารย์สอบสัมภาษณ์

9) สอบคัดเลือกนักศึกษาใหม่(รอบโควตา)

10) สอบคัดเลือกนักศึกษาใหม่(รอบรับตรง)

11) สอบสัมภาษณ์นักศึกษาใหม่(รอบโควตา)

12) สอบสัมภาษณ์นักศึกษาใหม่(รอบรับตรง)

13) จัดทำข้อสอบ

14) จัดทำคำสั่งต่าง ๆ งานรับสมัคร

15) ยืนยันสิทธิ์นักศึกษาใหม่

16) รับรายงานตัวนักศึกษาใหม่

17) ทำลายเอกสารข้อสอบ

18) จัดทำโครงการแนะแนวให้โอกาสทางการศึกษา
19) จัดประชุมอาจารย์แนะแนว
20) ออกแนะแนวการศึกษาต่อ
21) สแกนหลักฐานนักศึกษา
22) เก็บหลักฐานฐานนักศึกษา
23) ตรวจสอบคุณวุฒินักศึกษา
24) แจ้งผลการตรวจสอบคุณวุฒินักศึกษาที่สำเร็จการศึกษาแล้ว
25) โอนสภาพการเป็นนักศึกษาจากภาคปกติ เป็นภาคพิเศษ (กศ.ป.)
26) ขอย้ายสาขาวิชา
27) รับโอน ย้าย สถานศึกษา
28) ขอย้ายสถานศึกษา
29) ขอคืนสภาพ รักษาสภาพ และลาพักการเรียน
30) ขอลาออก
31) ขอเปลี่ยนชื่อ – นามสกุลนักศึกษา
32) กระบวนการเร่งรัดการชำระค่าเทอมนักศึกษา
33) ตรวจสอบพ้นสภาพการเป็นนักศึกษาโดยไม่ลงทะเบียนเรียน
34) ตรวจสอบพ้นสภาพการเป็นนักศึกษาโดยผลการเรียน
35) ทำลายเอกสารประวัตินักศึกษา
36) จัดทำบัตรประจำตัวนักศึกษา
37) จัดทำโครงการจัดทำบัตรประจำตัวนักศึกษาใหม่
38) จัดทำบัตรประจำตัวนักศึกษาใหม่ระดับปริญญาตรี/ป.โท/ป.เอก/ป.บัณฑิต
39) จัดทำบัตรประจำตัวนักศึกษา (กรณีบัตรสูญหาย ชำรุด หรือหมดอายุ)
40) จัดทำใบรับรองคุณวุฒิ (รอบอนุมัติผลการสำเร็จการศึกษา)
41) จัดทำใบแทนรับรองคุณวุฒิ (กรณีขอทำใหม่)
42) จัดทำใบรับรองคุณวุฒิ (ภาษาอังกฤษ)
43) จัดทำใบรายงานผลการเรียนชั่วคราว
44) จัดทำใบรับรองการเป็นนักศึกษา
45) จัดทำหนังสือรับรองผลการเรียน (ครบหลักสูตร)
46) จัดทำหนังสือรับรองการเรียน (รับรองหน่วยกิต)
47) จัดทำหนังสือรับรองการเรียน (หลักสูตรปริญญาตรี 5 ปี)
48) จัดทำใบทรานสคริป (รอบอนุมัติผลการสำเร็จการศึกษา)

49) จัดทำใบทรานสคริป (กรณีขอทำใหม่)
50) จัดทำใบทรานสคริป (ภาษาอังกฤษ)
51) จัดทำเอกสารการขอ Digital Transcript
52) จัดทำใบปริญญาบัตร (รอบรับปริญญา)
53) จัดทำใบแทนปริญญาบัตร (กรณีขอทำใหม่)
54) จัดทำใบปริญญาบัตร (ภาษาอังกฤษ)
55) ขออนุมัติผลการสำเร็จการศึกษา(รอบอนุมัติผล)
56) ขออนุมัติผลการสำเร็จการศึกษา(กรณีนักศึกษาตกค้าง)
57) งานทะเบียนหลักสูตรระยะสั้น
58) งานให้บริการหน้าเคาน์เตอร์ และด้านอื่น ๆ แก่ผู้มาติดต่อ
59) งานอื่น ๆ ที่ได้รับหมอบหมาย

งานบริการการศึกษาและสารสนเทศ หน้าที่รับผิดชอบ

1) ตรวจสอบการจัดทำรายวิชา 7 หลักสูตร ต่อปีหลักสูตรละ ประมาณ 70 รายวิชา
2) จัดทำแผนการเรียนนักศึกษาใหม่
3) สำรวจและยืนยันแผนการเรียน
4) แก้ไขแผนการเรียน
5) ลงทะเบียนวิชาเลือกเสรี
6) สำรวจตารางสอน
7) จัดตารางสอน
8) แก้ไขตารางสอน
9) ตรวจสอบการเบิกค่าตอบแทนรายชั่วโมงจำนวน
10) สำรวจตารางสอบ
11) จัดตารางสอบ
12) บรรยายให้ความรู้เรื่องการเทียบโอนรายวิชาสำหรับ นศ.ใหม่
13) การเทียบรายวิชาหลักสูตร 4 ปี (จบ ปวส.)
14) เทียบโอนรายวิชาสำหรับนักศึกษาที่เรียนมาจากสถาบันการศึกษาอื่น
15) ตรวจสอบการเรียนครบหลักสูตร
16) ให้บริการสืบค้นคำอธิบายรายวิชา
17) งานอื่น ๆ ที่ได้รับมอบหมาย
18) จัดทำโครงการเกี่ยวกับระบบสารสนเทศ

19) ปรับปรุงแก้ไขระบบรับสมัครนักศึกษา (รอบโควตา)
20) พัฒนา/ปรับปรุงระบบจัดเก็บข้อมูลเอกสาร
21) ปรับปรุงระบบบันทึกข้อมูลการชำระเงินผ่านธนาคาร ปณท.
22) จัดการข้อมูลลงทะเบียน นศ. กยศ. และ E_AUDIT
23) ปรับปรุงวางแผนโครงสร้างพื้นฐานด้านเครือข่ายภายในและเครื่องแม่ข่ายที่ให้บริการ
24) ปรับปรุงแก้ไขโปรแกรมตามข้อเสนอแนะของผู้ใช้ระบบ
25) ปรับปรุงข้อมูลระบบบริหารการศึกษาให้เป็นปัจจุบันเพื่อทำการเผยแพร่
26) ซ่อมบำรุงอุปกรณ์
27) ติดตั้งระบบรับรายงานตัวนักศึกษาใหม่
28) ปรับปรุงข้อมูลข่าวสารบนเว็บไซต์หน่วยงาน
29) จัดทำรายงานสถิติต่าง ๆ
30) จัดทำข้อมูลผู้สำเร็จการศึกษาส่งสำนักงานคณะกรรมการการอุดมศึกษา
31) ตรวจข้อสอบนักศึกษา รายวิชาหมวดวิชาศึกษาทั่วไป
32) บันทึกข้อมูลและการจัดเก็บเอกสารขอเลื่อนส่งผลการเรียน
33) การติดตามการส่งผลการเรียนของอาจารย์ผู้สอน
34) การเสนอขออนุมัติผ่อนผันการลงทะเบียน
35) การกลั่นกรองผลการเรียนแบบระบบเก่า
36) การกลั่นกรองผลการเรียนแบบระบบออนไลน์
37) การขอยกเลิกรายวิชา
38) การจัดเก็บเอกสารการขอยกเลิกรายวิชา
39) การปรับกลุ่มรายวิชา
40) การเปลี่ยน section
41) การถอนรายวิชา
42) การจัดเก็บเอกสารการเพิ่ม/ถอนรายวิชา
43) การเปลี่ยนค่าระดับคะแนน
44) การจัดเก็บเอกสารการเปลี่ยนค่าระดับคะแนน
45) การจัดทำแฟ้มผู้สอนสำหรับเปิดภาคเรียน
46) รับและบันทึกการส่งผลการเรียนระบบออนไลน์
47) รับผลการเรียนระบบเก่า(เกรดชีท)
48) การแก้ไขผลการเรียนกรณีผู้สอนบันทึกข้อมูลไม่ถูกต้อง
49) ปรับผลการเรียนจาก I เป็น F

50) การเก็บหลักฐานผลการเรียนเข้าแฟ้ม (ทุกรายวิชา)

51) แจ้งผลการเรียนให้ผู้ปกครองของนักศึกษารับทราบ

52) งานให้บริการด้านอื่น ๆ แก่ผู้มาติดต่อ

งานหลักสูตรและมาตรฐานทางการศึกษา หน้าที่ความรับผิดชอบ

1) การพัฒนา/ปรับปรุง/เปลี่ยนแปลง/ปิดหลักสูตร ระดับปริญญาตรี

2) ศึกษากรอบมาตรฐานคุณวุฒิอุดมศึกษาแห่งชาติ

3) ศึกษาเกณฑ์มาตรฐานคุณวุฒิระดับปริญญาตรี

4) กระบวนการนำเสนอหลักสูตร (มคอ.2) เพื่อพิจารณาอนุมัติ(พัฒนา/ปรับปรุงหลักสูตรระดับปริญญาตรี)

5) ติดตามผลการดำเนินงานตามตัวบ่งชี้ของหลักสูตรระดับปริญญาตรี (มาตรฐานหลักสูตร)

6) ประกันคุณภาพการศึกษาการบริหารจัดการหลักสูตรระดับมหาวิทยาลัยร่วมกับบัณฑิตและงานประกันคุณภาพการศึกษามหาวิทยาลัย (1.1 และ 5.3)

7) กระบวนการนำเสนอขอปิดหลักสูตรเพื่อพิจารณา (ปิดหลักสูตร)

8) ติดต่อประสานงาน ติดตามการรับทราบการเห็นชอบหลักสูตร/ปิดหลักสูตร จากสำนักงานปลัดกระทรวงอุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.)

9) กระบวนการนำเสนอการแก้ไขเปลี่ยนแปลงอาจารย์ผู้รับผิดชอบหลักสูตรอาจารย์ประจำหลักสูตร (สมอ.08)

10) ติดต่อประสานงานติดตามการแก้ไขเปลี่ยนแปลงอาจารย์ผู้รับผิดชอบหลักสูตร,อาจารย์ประจำหลักสูตร (สมอ.08) กับสำนักงานปลัดกระทรวง อุดมศึกษาวิทยาศาสตร์ วิจัยและนวัตกรรม (สป.อว.)

11) Admin ระบบพิจารณาความสอดคล้องของหลักสูตรระดับอุดมศึกษา (CHE Curriculum Online : CHECO)

12) ติดต่อประสานงานการรับทราบหลักสูตร จากสำนักงานคณะกรรมการข้าราชการครูและบุคลากรทางการศึกษา (ก.ค.ศ.)

13) ติดต่อประสานงานการรับทราบหลักสูตร จากสำนักงานคณะกรรมการข้าราชการพลเรือน (ก.พ.)

14) ติดต่อประสานงานการรับทราบหลักสูตร จากกองทุนเงินให้กู้ยืมเพื่อการศึกษา (กยศ.)

15) กลั่นกรองรูปแบบหลักสูตรระดับปริญญาตรี (มคอ.2)

16) ร่าง - พิมพ์ ,รับ - ส่ง หนังสือราชการภายใน ภายนอก คำสั่ง ประกาศ ที่เกี่ยวข้องกับงานที่รับผิดชอบ

17) ดำเนินการประสานงานการปรับปรุง หมวดวิชาศึกษาทั่วไป

18) จัดทำงบประมาณ ชุดเอกสารการเบิกจ่าย ค่าวัสดุ ค่าตอบแทนวิทยากร ค่าจ้างเหมาบริการ ค่าใช้จ่ายในการเดินทางไปราชการ ค่าตอบแทนปฏิบัติงานนอกเวลาราชการ ยืมเงินทดรองจ่ายราชการ

19) รายงานผลการดำเนินงานตามโครงการที่รับผิดชอบ

20) ดำเนินการจัดประชุม คณะกรรมการบริหารหมวดวิชาศึกษาทั่วไป คณะกรรมการบริหารรายวิชาศึกษาทั่วไป รวมถึงคณาจารย์ผู้สอนรายวิชาศึกษาทั่วไป เช่น ทำบันทึกขอเชิญประชุม รวบรวมทำเล่มวาระการประชุม จองห้องประชุม เตรียมอาหารว่างและเครื่องดื่ม และบันทึกรายงานการประชุมที่ เกี่ยวข้องกับงานที่รับผิดชอบ

21) ดำเนินการติดตามขอความร่วมมือประธานกรรมการบริหารรายวิชากรอกรายละเอียดของรายวิชา (มคอ.3) พร้อมรายงานผลการดำเนินงานของรายวิชา (มคอ.5)

22) ติดตามขอความร่วมมือประชาสัมพันธ์ให้นักศึกษาประเมินผู้สอนในแบบ ทส.01 รายวิชาศึกษาทั่วไป

23) ดำเนินการทวนสอบผลสัมฤทธิ์ตามมาตรฐานการเรียนรู้หมวดวิชาศึกษาทั่วไปในแต่ละปีการศึกษา

24) หนังสือราชการหลักสูตรระยะสั้น

25) งานจัดประชุม ร่างวาระการประชุมและสรุปวาระการประชุมที่เกี่ยวข้องกับงานหลักสูตรอบรมระยะสั้น และสรุปรายงานการประชุมของสำนักฯ

26) งานการเงินและพัสดุ

27) จัดทำชุดเบิกจ่าย (พด.) เกี่ยวกับโครงการที่รับผิดชอบ

28) การยืมเงินทดรองราชการงานตรวจสอบการรายงานการเดินทางไปราชการที่เกี่ยวข้องกับงานหลักสูตรอบรมระยะสั้น

29) ประสานงานทั้งหน่วยงานภายใน และภายนอก

30) วางแผนการดำเนินงานโครงการ

31) จัดเตรียมเอกสาร อาหาร อาหารว่างและเครื่องดื่ม ระหว่างการฝึกอบรม

32) เสนอแต่งตั้งคณะทำงาน คณะกรรมการ ประสานงานที่เกี่ยวข้องกับงานหลักสูตรอบรมระยะสั้นให้กับนักศึกษา

33) จัดอบรมสัมมนาให้ความรู้แก่อาจารย์เกี่ยวกับหลักสูตรระยะสั้น

34) ทำหน้าที่ประสานงานและอำนวยความสะดวกแก่อาจารย์ และผู้เข้าร่วมอบรมหลักสูตรอบรมระยะสั้น

งานส่งเสริมและพัฒนาวิชาการ หน้าที่ความรับผิดชอบ

1) ลงทะเบียนรับ – ส่งหนังสือภายในและภายนอกมหาวิทยาลัย

2) กลั่นกรองและพิจารณาเอกสารหลักฐานที่เกี่ยวข้อง

3) ประสานงานผู้ทรงคุณวุฒิพิจารณาตำแหน่งทางวิชาการ

4) จัดประชุมคณะอนุกรรมการประเมินผลการสอนและคุณภาพทางวิชาการเพื่อขอกำหนดตำแหน่งทางวิชาการ

5) จัดประชุมอนุกรรมการพิจารณาตรวจสอบและกลั่นกรองผลงานทางวิชาการ

6) จัดประชุมคณะกรรมการผู้ทรงคุณวุฒิประเมินผลงานทางวิชาการและประเมินจริยธรรมและจรรยาบรรณทางวิชาการ

7) จัดประชุมคณะกรรมการพิจารณาตำแหน่งทางวิชาการ

8) จัดทำเอกสารเกี่ยวกับการจ่ายค่าตอบแทนผู้ทรงคุณวุฒิ และค่าใช้จ่ายอื่น ๆ

9) Admin ระบบติดตามความก้าวหน้าในการขอกำหนดตำแหน่งทางวิชาการ

10) Admin ระบบทำเนียบผู้ดำรงตำแหน่งทางวิชาแห่งชาติ

11) จัดประชุมสำนักส่งเสริมวิชาการและงานทะเบียนและกรรมการบริหารสำนักฯ

12) ปฏิบัติงานเกี่ยวกับการงานด้านธุรการ และงานสารบรรณ งานเอกสารการพิมพ์ งานประชุม งานพัสดุ งานการเงิน (เบิกจ่ายค่าตอบแทน) งานงบประมาณ ที่เกี่ยวข้องดำเนินงานด้านสหกิจศึกษาและการศึกษาเชิงบูรณาการ(CWIE) วิชาเลือกเสรี ลำนักพิมพ์ฯ

13) ประสานงานจัดเก็บข้อมูล และรายงานผลการดำเนินงานด้านสหกิจศึกษาและการศึกษาเชิงบูรณาการ (CWIE)

14) จัดทำติดตามและรายงานผลโครงการที่รับผิดชอบ

15) จัดเก็บข้อมูลการประกันคุณภาพการศึกษาภายใน ระดับหาวิทยาลัย:องค์ประกอบที่ 5 การบริหารจัดการตัวบ่งชี้ที่ 5.4 การจัดการเรียนรู้แบบบูรณาการกับการทำงาน

16) จัดทำคู่มือและแบบฟอร์มต่าง ๆ ของงานสหกิจศึกษา

17) จัดทำฐานข้อมูลสถานประกอบการหรือหน่วยงาน เกี่ยวกับนักศึกษาสหกิจศึกษาและการศึกษาเชิงบูรณาการกับการทำงาน (CWIE)

18) ประสานงานกับหน่วยงานภาย – ภายนอก ในการจัดเก็บฐานข้อมูลสหกิจศึกษาและการศึกษาเชิงบูรณาการกับการทำงาน (CWIE)

19) การสำรวจความคิดเห็นของนักศึกษาภาคปกติเกี่ยวกับการจัดการเรียนการสอนของอาจารย์มหาวิทยาลัยราชภัฏสกลนคร แต่ละภาคเรียน

20) ประสานงานกับเครือข่ายสหกิจ ภาคตะวันออกเฉียงเหนือ เกี่ยวกับการดำเนินงานสหกิจและการเชิงบูรณาการกับการทำงาน

21) งานลงนามในบันทึกความเข้าใจ (MOU), บันทึกข้อตกลง (MOA)

22) บริหารจัดการงบประมาณสำนักพิมพ์มหาวิทยาลัยราชภัฏสกลนคร

23) ดำเนินการจัดเก็บเอกสารสำนักพิมพ์มหาวิทยาลัยราชภัฏสกลนคร ให้เป็นระเบียบเรียบร้อย

24) จัดประชุมคณะกรรมการบริหารสำนักพิมพ์มหาวิทยาลัยราชภัฏสกลนคร

25) ประสานงานกับผู้สร้างสรรค์ผลงาน ในการส่งวรรณกรรมเพื่อขอให้พิจารณาจัดพิมพ์วรรณกรรม

26) จัดทำคำสั่งแต่งตั้งคณะกรรมการผู้ทรงคุณวุฒิเพื่อประเมินคุณภาพวรรณกรรม

27) ดำเนินการประสานงานกับผู้ทรงคุณวุฒิในการจัดส่งวรรณกรรม ให้กับผู้ทรงคุณวุฒิเพื่อพิจารณาวรรณกรรมของผู้สร้างสรรค์ผลงาน

28) ดำเนินการการตรวจสอบการคัดลอกผลงานด้วยโปรแกรมคอมพิวเตอร์ (อักขราวิสุทธิ์)

29) ปฏิบัติหน้าที่อื่น ๆ ที่มหาวิทยาลัยมอบหมาย

2. บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง

2.1 หน้าที่ความรับผิดชอบของตำแหน่งตามมาตรฐานกำหนดตำแหน่ง

ตามมาตรฐานกำหนดตำแหน่งสายงานนักวิชาการคอมพิวเตอร์ ที่กำหนดโดย ก.พ.อ. เมื่อวันที่ 21 กันยายน 2553 ระบุบทบาทหน้าที่ความรับผิดชอบของสายงานนักวิชาการคอมพิวเตอร์ ระดับปฏิบัติการ ดังนี้

2.1.1 หน้าที่ความรับผิดชอบหลัก

ปฏิบัติงานในฐานะผู้ปฏิบัติงานระดับต้นที่ต้องใช้ความรู้ความสามารถทางวิชาการในการทำงานปฏิบัติงานเกี่ยวกับคอมพิวเตอร์ ภายใต้การกำกับ แนะนำ ตรวจสอบ และปฏิบัติงานอื่นตามที่ได้รับมอบหมาย โดยมีลักษณะงานที่ปฏิบัติในด้านต่างๆ ดังนี้

1) ด้านการปฏิบัติการ

ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ที่เกี่ยวข้อง ติดตั้งเครื่องแม่ข่ายคอมพิวเตอร์และทดสอบคุณสมบัติด้านเทคนิคของระบบ ติดตั้งชุดคำสั่งระบบปฏิบัติการ ชุดคำสั่งสำเร็จรูป เพื่ออำนวยการให้งานเทคโนโลยีสารสนเทศในความรับผิดชอบดำเนินไปได้อย่างราบรื่นและสอดคล้องกับความต้องการของหน่วยงาน

ประมวลผล และประปรุงแก้ไขแฟ้มข้อมูล เขียนชุดคำสั่ง และคู่มือคำอธิบายชุดคำสั่งตามข้อกำหนดของระบบงานที่ได้วางแผนไว้แล้ว ทดสอบความถูกต้องของคำสั่ง แก้ไขข้อผิดพลาดของคำสั่ง เพื่อให้ระบบปฏิบัติการทำงานได้อย่างถูกต้องแม่นยำและมีประสิทธิภาพมากที่สุด

ให้บริการวิชาการด้านต่างๆ เช่น ช่วยสอน ถ่ายทอดเทคโนโลยีในสาขาวิทยาการคอมพิวเตอร์ให้คำปรึกษา แนะนำในการปฏิบัติงานแก่เจ้าหน้าที่ระดับลองลงมาและแก่นักศึกษาที่มาฝึกปฏิบัติงาน ตอบปัญหาและชี้แจงเรื่องต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง มีประสิทธิภาพ และปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง

2) ด้านการวางแผน

วางแผนการทำงานที่รับผิดชอบ ร่วมวางแผนการทำงานของหน่วยงานหรือโครงการเพื่อให้การดำเนินงานบรรลุตามเป้าหมายและผลสัมฤทธิ์ที่กำหนด

3) ด้านการประสานงาน

ประสานการทำงานร่วมกันระหว่างทีมงานหรือหน่วยงานทั้งภายในและภายนอกเพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้

ชี้แจงและให้รายละเอียดเกี่ยวกับข้อมูล ข้อเท็จจริง แก่บุคคลหรือหน่วยงานที่เกี่ยวข้องเพื่อสร้างความเข้าใจหรือความร่วมมือมนการดำเนินงานตามที่ได้รับมอบหมาย

4) ด้านการบริการ

ให้คำปรึกษา แนะนำเบื้องต้น เผยแพร่ ถ่ายทอดความรู้ ทางด้านวิทยาการคอมพิวเตอร์รวมทั้งตอบปัญหาและชี้แจงเรื่องต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้ผู้รับบริการได้รับข้อมูลความรู้ต่างๆ ที่เป็นประโยชน์

จัดเก็บข้อมูลเบื้องต้น และให้บริการข้อมูลทางวิชาการ เกี่ยวกับด้านวิชาการคอมพิวเตอร์เพื่อให้บุคลากรทั้งภายในและภายนอกหน่วยงาน นักศึกษา ตลอดจนผู้รับบริการได้ทราบข้อมูลและความรู้ต่างๆ ที่เป็นประโยชน์ สอดคล้อง และสนับสนุนภารกิจของหน่วยงานและใช้ประกอบการพิจารณากำหนดนโยบาย แผนงาน หลักเกณฑ์ มาตรการต่างๆ

2.2 หน้าที่ความรับผิดชอบของตำแหน่งตามที่ได้รับมอบหมาย

บทบาทหน้าที่ความรับผิดชอบของนายวงเวียน วงค์กะโซ่ ตำแหน่งนักวิชาการคอมพิวเตอร์ ระดับ ปฏิบัติการ ตามที่ได้รับมอบหมาย มีดังนี้

2.2.1 พัฒนาระบบบริหารการศึกษา ในส่วนของเจ้าหน้าที่และนักศึกษา เพื่อรองรับกระบวนการที่เกี่ยวข้องกับการจัดการเรียนการสอน

2.2.2 พัฒนาระบบสมัครเรียนออนไลน์ เพื่อให้นักเรียน สามารถสมัครและชำระเงินผ่านธนาคาร

2.2.3 ติดตั้งและดูแลเครื่องแม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศของสำนักส่งเสริมวิชาการและงานทะเบียน

2.2.4 สำรองข้อมูลระบบบริหารการศึกษาระบบงานทะเบียนนักศึกษา

2.2.5 พัฒนาระบบบริหารการศึกษา ในส่วนของอาจารย์ผู้สอน เพื่อให้ผู้สอนสามารถเข้าถึงสารสนเทศได้ในรูปแบบออนไลน์ สามารถตรวจสอบผลการเรียนของนักศึกษา พิมพ์รายชื่อนักศึกษาในรายวิชา และอื่นที่เกี่ยวข้อง

2.2.6 พัฒนาระบบส่งผลการเรียนออนไลน์ เพื่ออำนวยความสะดวกให้อาจารย์ผู้สอนบันทึกคะแนนและประมวลผลการเรียนผ่านระบบโดยอัตโนมัติ สามารถติดตามสถานะการส่งเกรดได้อย่างมีประสิทธิภาพ

2.2.7 พัฒนาระบบและวิเคราะห์ข้อมูลการประเมินผลการจัดการเรียนการสอนออนไลน์ โดยให้นักศึกษาสามารถประเมินได้ผ่านระบบออนไลน์

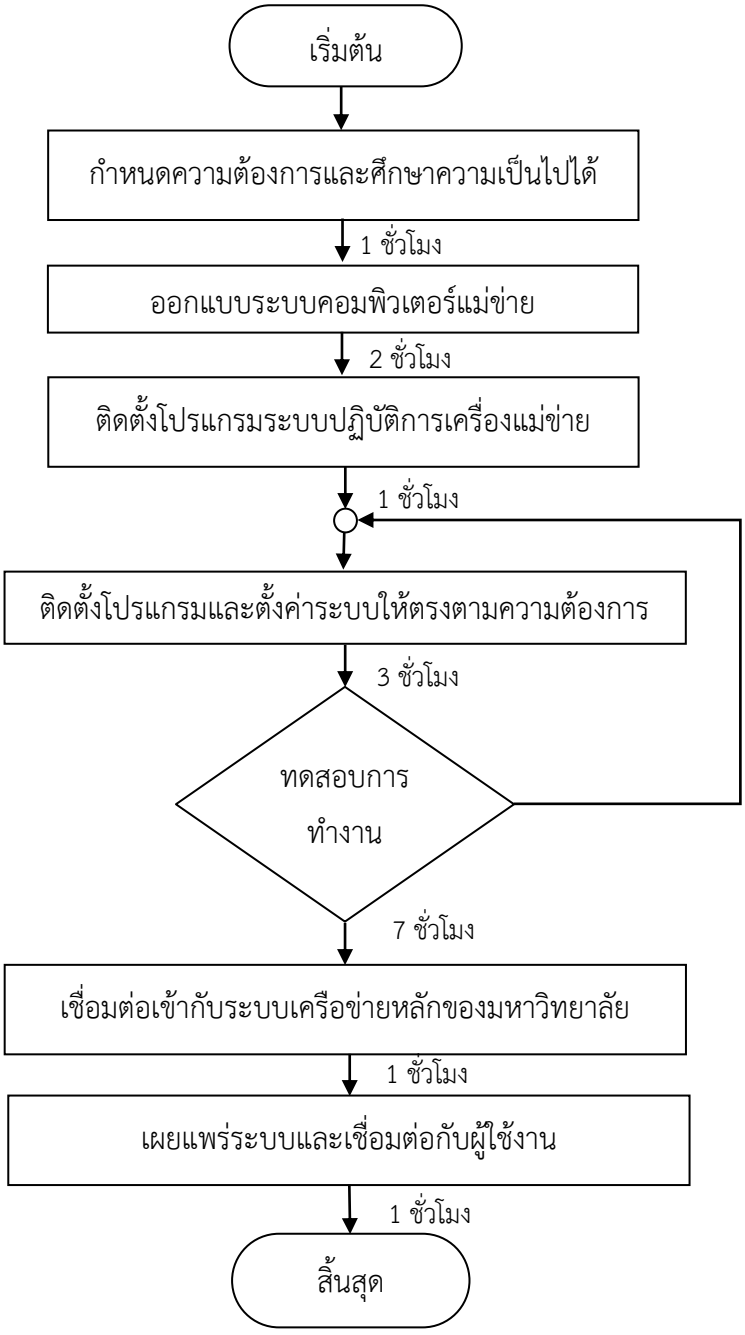
2.2.8 พัฒนาระบบสารสนเทศเพื่อจัดเก็บข้อมูลหลักสูตรของมหาวิทยาลัยราชภัฏสกลนคร ให้สอดคล้องกับ มคอ.

2.2.9 สำรองข้อมูลและดูแลระบบฐานข้อมูลระบบงานทะเบียนนักศึกษา

2.2.10 พัฒนาระบบจองการระบบจัดการ Zoom License มหาวิทยาลัยราชภัฏสกลนคร

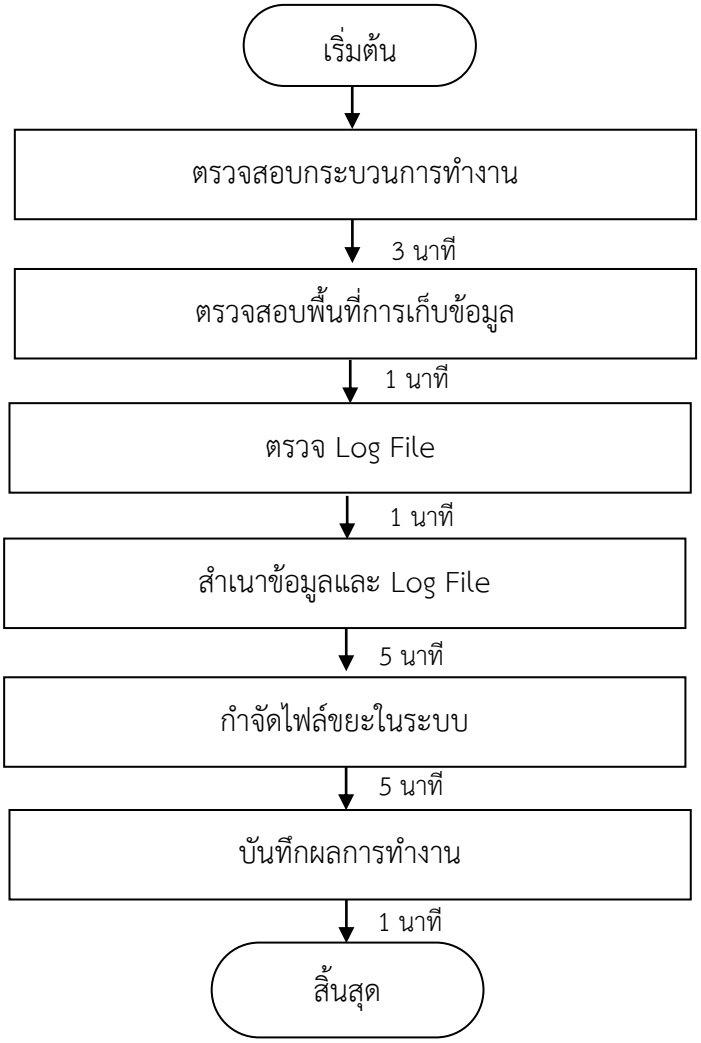
จากภาระหน้าที่ที่ได้รับมอบหมายดังกล่าวข้างต้น ผู้เขียนได้เลือกเอาภาระงานติดตั้งและดูแลเครื่องแม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศของสำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร มาเขียนคู่มือการปฏิบัติงาน โดยมี Flow Chart ดังนี้

ขั้นตอนการติดตั้งระบบคอมพิวเตอร์แม่ข่าย
สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร



ภาพประกอบ 4 ขั้นตอนการติดตั้งระบบคอมพิวเตอร์แม่ข่าย

ขั้นตอนการดูแลระบบคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน



ภาพประกอบ 5 ขั้นตอนการดูแลระบบคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน

บทที่ 3

หลักเกณฑ์วิธีการปฏิบัติงาน

ในการปฏิบัติงานตามคู่มือเรื่อง การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร มีหลักเกณฑ์ที่เกี่ยวข้องดังนี้

ใช้หลักปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร พ.ศ. 2557 ซึ่งได้กำหนดวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งนโยบายออกเป็นส่วนๆ ดังต่อไปนี้

ส่วนที่ 1 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

เป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการ เข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานที่เป็นบุคลากรของมหาวิทยาลัย และบุคคลภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

ส่วนที่ 2 แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

แนวทางสำหรับผู้ใช้งานที่เป็นบุคลากรของมหาวิทยาลัยและบุคคลภายนอก ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของมหาวิทยาลัยให้เป็นความลับ มีความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

ส่วนที่ 3 แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

เป็นมาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายของมหาวิทยาลัย และ ป้องกันการบุกรุกผ่านระบบเครือข่าย หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายกับข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวตนที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของมหาวิทยาลัยได้อย่างถูกต้อง

ส่วนที่ 4 แนวปฏิบัติของผู้ดูแลระบบ

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบ (System Administrator) ในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย (Network) ให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลผู้ใช้งานให้เป็นไปตามแนวนโยบาย

ส่วนที่ 5 แนวปฏิบัติการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำ หน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมในกรณีเกิดเหตุฉุกเฉินหรือไม่สามารถดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์ ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งาน ระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของ มหาวิทยาลัย

ส่วนที่ 6 แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้าน สารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่าง ชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

ส่วนที่ 7 แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยี สารสนเทศ

กล่าวเกี่ยวกับแนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้องได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนาไปปฏิบัติ ได้อย่างถูกต้อง

ส่วนที่ 8 การกำหนดผู้รับผิดชอบ

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรือ อันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตาม แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

บทบาทที่สำคัญและซอฟต์แวร์ที่จำเป็นสำหรับเครื่องแม่ข่ายคอมพิวเตอร์

1.เครื่องแม่ข่าย (Server)

เครื่องแม่ข่าย หรือ Server คือเครื่องคอมพิวเตอร์ที่ออกแบบมาเพื่อให้บริการแก่เครื่องคอมพิวเตอร์อื่นๆ (Client) ในเครือข่าย โดยทำหน้าที่เป็นศูนย์กลางในการจัดเก็บข้อมูล ประมวลผล และแบ่งปันทรัพยากรต่างๆ

1.1 ความสำคัญของเครื่องแม่ข่ายในสถาบันการศึกษา

- จัดเก็บและจัดการข้อมูลนักศึกษา ข้อมูลวิชาการ และข้อมูลทะเบียน
- รองรับระบบสารสนเทศต่างๆ ของมหาวิทยาลัย
- ให้บริการเว็บไซต์ อีเมล และระบบออนไลน์
- สำรองข้อมูลและรักษาความปลอดภัย

2. ประเภทของเครื่องแม่ข่าย

2.1 จำแนกตามการใช้งาน

2.1.1 Web Server (เว็บเซิร์ฟเวอร์)

- หน้าที่: ให้บริการเว็บไซต์และเว็บแอปพลิเคชัน
- ซอฟต์แวร์: Apache, Nginx, IIS
- การใช้งานในมหาวิทยาลัย: เว็บไซต์หลัก, ระบบลงทะเบียนออนไลน์

2.1.2 Database Server (เซิร์ฟเวอร์ฐานข้อมูล)

- หน้าที่: จัดเก็บและจัดการฐานข้อมูล
- ซอฟต์แวร์: MySQL, PostgreSQL, Microsoft SQL Server, Oracle
- การใช้งานในมหาวิทยาลัย: ฐานข้อมูลนักศึกษา, ระบบทะเบียน, ข้อมูลวิชาการ

2.1.3 File Server (เซิร์ฟเวอร์ไฟล์)

- หน้าที่: จัดเก็บและแบ่งปันไฟล์
- ระบบ: Windows File Server, Samba, FTP Server
- การใช้งานในมหาวิทยาลัย: เก็บเอกสาร, แบ่งปันไฟล์งาน

2.1.4 Application Server (เซิร์ฟเวอร์แอปพลิเคชัน)

- หน้าที่: รันโปรแกรมและแอปพลิเคชันต่างๆ
- เทคโนโลยี: Java EE, .NET, PHP
- การใช้งานในมหาวิทยาลัย: ระบบสารสนเทศ, ระบบบริหารจัดการ

หลักปฏิบัติงานที่สำคัญในการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร

1 การกำหนดเลข IP Address สำหรับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งหมายเลข IP Address ที่สำนักส่งเสริมวิชาการและงานทะเบียน ได้รับจัดสรรมาจำนวน 253 หมายเลข (172.16.1.1 – 253) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร

2 การจัดเตรียมอุปกรณ์ในส่วนที่เป็นฮาร์ดแวร์เพื่อวางแผนการติดตั้งแม่ข่ายคอมพิวเตอร์ ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server Computer) เครื่องกระจายสัญญาณระบบเครือข่าย (Switching HUB) สายสัญญาณ (UTP Cable)

2.1 คู่มือนี้จะแสดงการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายโดยใช้ Server Computer จำนวน 3 เครื่อง เพื่อติดตั้งแม่ข่ายให้บริการดังนี้ ระบบ SNRU Connect (1) Database Server สำหรับฐานข้อมูลระบบบริหารการศึกษา (2) Web Server ระบบสนับสนุนการจัดการเรียนการสอน (Apache Web server) (3) Web Server สำหรับระบบบริหารการศึกษา(IIS Web Server) ระบบ SNRU Connect

2.2 วางแผนการติดตั้งแม่ข่ายดังนี้

2.2.1 เครื่องคอมพิวเตอร์แม่ข่าย เครื่องที่ 1 ดาต้าเบสเซิร์ฟเวอร์ สำหรับฐานข้อมูลระบบบริหารการศึกษา กำหนดหมายเลข IP Address: 172.16.1.200
Subnet Mask: 255.255.255.0 Default Gateway: 172.16.1.254 Preferred DNS Server: 202.29.24.10 Alternate DNS Server: 10.8.8.10

2.2.2 เครื่องคอมพิวเตอร์แม่ข่าย เครื่องที่ 2 เว็บเซิร์ฟเวอร์ ระบบสนับสนุนการจัดการเรียนการสอน (Apache Web server) กำหนดหมายเลข IP Address: 172.16.1.247 Subnet Mask: 255.255.255.0 Default Gateway: 172.16.1.254 Preferred DNS Server: 202.29.24.10 Alternate DNS Server: 10.8.8.10

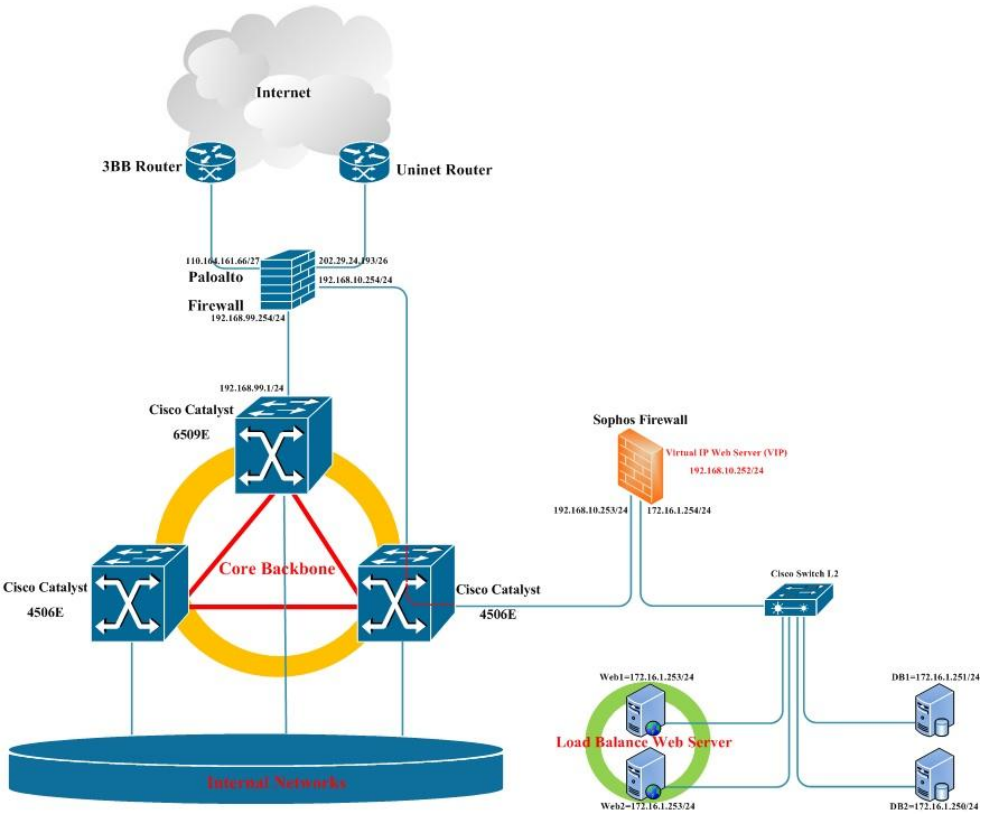
2.2.3 เครื่องคอมพิวเตอร์แม่ข่าย เครื่องที่ 3 เว็บเซิร์ฟเวอร์ สำหรับระบบบริหารการศึกษา (IIS Web Server) ระบบ SNRU Connect กำหนดหมายเลข IP Address: 172.16.1.247 Subnet Mask: 255.255.255.0 Default Gateway: 172.16.1.254 Preferred DNS Server: 202.29.24.10 Alternate DNS Server: 10.8.8.10

3 การเชื่อมต่อเครื่องกระจายสัญญาณระบบเครือข่าย

เครื่องกระจายสัญญาณที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร ได้ทำการติดตั้งสำหรับสำนักส่งเสริมวิชาการและงานทะเบียนเชื่อมต่อสัญญาณระบบเครือข่ายไปยัง ระบบเครือข่ายมหาวิทยาลัยมหาวิทยาลัยราชภัฏสกลนคร การปฏิบัติงานตามคู่มือนี้จะทำการเชื่อมต่อเครื่องแม่ข่ายคอมพิวเตอร์ 1, 2 เข้ากับเครื่องกระจายสัญญาณนี้ด้วยสายสัญญาณระบบเครือข่ายแบบ Unshielded Twisted pair (UTP) ชนิด CAT 6 ยกเว้นเครื่อง Server เครื่องที่ 3 จะอยู่ภายใต้เครื่อง 172.16.1.247 โดยทำงานในรูปแบบคอมพิวเตอร์เสมือน (Virtual Machine)

4 การเชื่อมต่อสายสัญญาณระบบเครือข่าย

การเชื่อมต่อระบบเครื่องคอมพิวเตอร์แม่ข่าย ของสำนักส่งเสริมวิชาการและงานทะเบียน เป็นการเชื่อมต่อโดยแยกโซนของการเข้าใช้งาน โดยจะไม่สามารถเข้าถึงได้โดยตรงจากภายนอก และจะมีการกำหนดให้ผู้ใช้งานทั่วไป สามารถใช้บริการผ่านโดเมนที่กำหนดให้เท่านั้น



ภาพประกอบ 6 ผังการเชื่อมต่อคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน

5 การดำเนินงานติดตั้งระบบภายใต้พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

มาตรา 16 ให้ยกเลิกความในมาตรา 22 มาตรา 23 มาตรา 24 และมาตรา 25 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน มาตรา 22 ห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามมาตรา 18 วรรคสอง เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มา ตามมาตรา 18 ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นในกรณีตามมาตรา 18 วรรคสอง หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบหรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่ตามมาตรา 18 วรรคสอง โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ มาตรา ๒๓ พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา 18 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 24 ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามมาตรา 18 และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจาคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 25 ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มา ตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา 18 วรรคสอง ให้อ้างและรับฟัง เป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วยการสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบ ประการอื่น

มาตรา 17 ให้ยกเลิกความในวรรคหนึ่งของมาตรา 26 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และให้ใช้ความต่อไปนี้แทน

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ข้อควรระวังในการปฏิบัติงาน

ในการปฏิบัติงานตามคู่มือเรื่อง การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร มีข้อควรระวังในการปฏิบัติงานดังนี้

1) การวางแผนและเตรียมการล่วงหน้า ควรศึกษารายละเอียดของระบบและขั้นตอนการติดตั้งอย่างละเอียดก่อนดำเนินการ เพื่อให้การติดตั้งเป็นไปอย่างราบรื่น
2) การสำรองข้อมูล ก่อนดำเนินการติดตั้งระบบใหม่ ควรสำรองข้อมูลสำคัญทั้งหมดไว้ก่อน เพื่อป้องกันการสูญหายของข้อมูล
3) การตรวจสอบอุปกรณ์และซอฟต์แวร์ ควรตรวจสอบให้แน่ใจว่าอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ที่จำเป็นสำหรับการติดตั้งระบบมีความเข้ากันได้และเพียงพอต่อความต้องการ
4) การติดตั้งโดยผู้เชี่ยวชาญ หากไม่มีความชำนาญในการติดตั้งระบบ ควรพิจารณาขอความช่วยเหลือจากผู้เชี่ยวชาญหรือผู้ให้บริการที่เกี่ยวข้อง เพื่อหลีกเลี่ยงปัญหาที่อาจเกิดขึ้นได้
5) การทดสอบระบบ หลังจากติดตั้งระบบเสร็จสิ้น ควรทดสอบการทำงานของระบบอย่างละเอียด เพื่อตรวจสอบว่าทุกส่วนทำงานได้อย่างถูกต้องและมีประสิทธิภาพ
6) การอัปเดตและปรับปรุงระบบ ระบบคอมพิวเตอร์จำเป็นต้องได้รับการอัปเดตและปรับปรุงอย่างสม่ำเสมอ เพื่อรักษาความปลอดภัยและประสิทธิภาพการทำงาน
7) การเชื่อมต่อสายสัญญาณระหว่าง Server Computer กับ Switching HUB ต้องเชื่อมต่อกับ Port ของ Server Computer ที่ได้กำหนดหมายเลข IP Address ไว้ให้ถูกต้อง มิเช่นนั้นจะทำให้เครื่องแม่ข่ายไม่สามารถเชื่อมต่อสัญญาณเข้ากับระบบเครือข่ายได้

8) การติดตั้ง การให้บริการ และการใช้งานใดๆ จะต้องไม่ละเมิดกฎหมาย ตามพระราชบัญญัติว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

โดยสรุป การวางแผน การเตรียมความพร้อม การตรวจสอบ และการปฏิบัติตามขั้นตอนอย่างระมัดระวังจะช่วยให้การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่ายเป็นไปอย่างราบรื่นและมีประสิทธิภาพ

บทที่ 4
เทคนิคการปฏิบัติงาน

กิจกรรม/แผนการปฏิบัติงาน

สำนักสงเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนครมีแนวโนมในการใชงานระบบสารสนเทศที่สูงและเติบโตมากขึ้นเรื่อย ๆ ซึ่งเป็นผลมาจากการที่มหาวิทยาลัยเปิดสาขาวิชาที่สอนมากขึ้นและรับนักศึกษาในแต่ละสาขาวิชาเพิ่มขึ้นมากกวาเดิมทำใหสำนักสงเสริมวิชาการและงานทะเบียนมีการ พัฒนาระบบสารสนเทศอย่างต่อเนื่องเพื่อตอบสนองต่อความตองการของผู้ใชที่เป็นนักศึกษา อาจารย เจาหนาที่และบุคลากรที่ช่วยในการบริหารจัดการงานต่าง ๆ ใหมีความสะดวกรวดเร็ว มากยิ่งขึ้น โดยเครื่องแม่ข่ายที่อยู่ในการควบคุมของสำนักสงเสริมวิชาการและงานทะเบียนมหาวิทยาลัยราชภัฏสกลนคร ตั้งอยู่ที่อาคารศูนย์ข้อมูล มหาวิทยาลัยราชภัฏสกลนคร (SNRU Data Center) ภายใต้การดูแลทางด้านกายภาพและสิ่งแวดล้อม ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร ได้แก่

- เครื่องแม่ข่าย ดาต้าเบสเซิร์ฟเวอร์ สำหรับฐานข้อมูลระบบบริหารการศึกษา
- เครื่องแม่ข่าย เว็บเซิร์ฟเวอร์ ระบบสนับสนุนการจัดการเรียนการสอน (Apache Web server)
- เครื่องแม่ข่าย เว็บเซิร์ฟเวอร์ สำหรับระบบบริหารการศึกษา (IIS Web Server) ระบบ SNRU Connect

เห็นได้ว่าสำนักสงเสริมวิชาการและงานทะเบียน มีการประยุกต์ใช้เครื่องคอมพิวเตอร์แม่ข่ายที่หลากหลาย เพื่อรองรับการทำงานที่หลากหลาย หากในอนาคตมีความจำเป็นต้องการใช้งานที่เพิ่มขึ้น ก็จำเป็นต้องเพิ่มจำนวนเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นการสิ้นเปลืองทรัพยากรและพลังงานไฟฟ้าในระยะยาว ผู้เขียนจึงได้นำเอาความสามารถในการจัดการทรัพยากรของ VirtualBox ซึ่งเป็นซอฟต์แวร์สำหรับสร้างระบบปฏิบัติการเสมือน (Virtual Machine) มาใช้ในการสร้างเครื่องแม่ข่ายเสมือนเพื่อให้บริการต่างๆ ภายในองค์กร

การใช้ VirtualBox ช่วยให้สามารถจัดสรรทรัพยากรคอมพิวเตอร์ เช่น หน่วยประมวลผล หน่วยความจำ พื้นที่จัดเก็บข้อมูล ได้อย่างยืดหยุ่น โดยไม่จำเป็นต้องมีเครื่องกายภาพจริงจำนวนมาก ทำให้ลดภาระในการบริหารจัดการและบำรุงรักษาฮาร์ดแวร์ จึงเป็นทางเลือกที่น่าสนใจสำหรับการจัดการระบบเครื่องแม่ข่ายภายในองค์กร โดยมีแผนการปฏิบัติงานดังนี้

ตารางแผนการปฏิบัติงาน

กิจกรรม	งบประมาณ พ.ศ. 2567											
	ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.
จัดเตรียมความพร้อมของอุปกรณ์	←	→										
ดำเนินการติดตั้งระบบ		←	→									
ทดสอบระบบ				←	→	→						
เปิดใช้งานระบบ							←	→	→	→	→	→
ตรวจสอบการทำงานให้สามารถใช้งานได้อย่างมีประสิทธิภาพ							←	→	→	→	→	→

เทคนิคการปฏิบัติงาน

การติดตั้งระบบปฏิบัติการ Windows Server บนคอมพิวเตอร์แม่ข่าย

คู่มือนี้จะแสดงการติดตั้งระบบปฏิบัติการ Microsoft Windows Server 2019 บนเครื่องคอมพิวเตอร์ Dell PowerEdge R730 ซึ่งใช้เป็นเครื่องคอมพิวเตอร์แม่ข่ายประจำอยู่ที่อาคารศูนย์ข้อมูล มหาวิทยาลัยราชภัฏสกลนคร (SNRU Data Center) มีขั้นตอนดังนี้

การติดตั้งระบบปฏิบัติการ Windows Server 2019 โดยใช้ CD/DVD

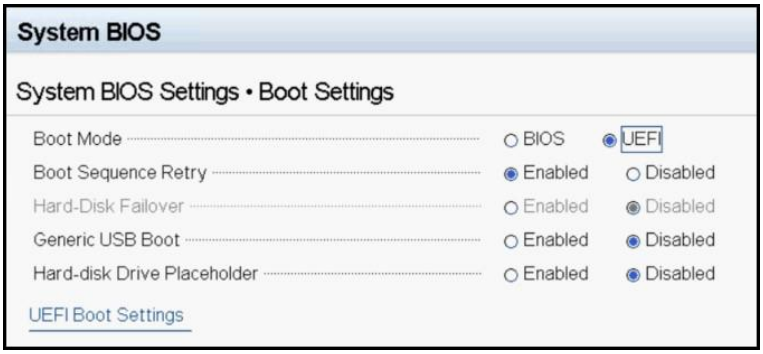
1. เชื่อมต่อแป้นพิมพ์ จอภาพ เมาส์ และอุปกรณ์ต่อพ่วงที่จำเป็นอื่นๆ เข้ากับระบบ
2. เปิดระบบและอุปกรณ์ต่อพ่วงที่เชื่อมต่อ
3. กด F2 เพื่อไปที่หน้าการตั้งค่าระบบ

ภาพประกอบ 7 ติดตั้งระบบ

4. บนหน้าจอ System Setup ให้คลิก System BIOS แล้วคลิก Boot Settings.

ภาพประกอบ 8 เมนูหลักของการตั้งค่าระบบ

5. ตรวจสอบให้แน่ใจว่าได้เลือก UEFI เป็นโหมดบูต

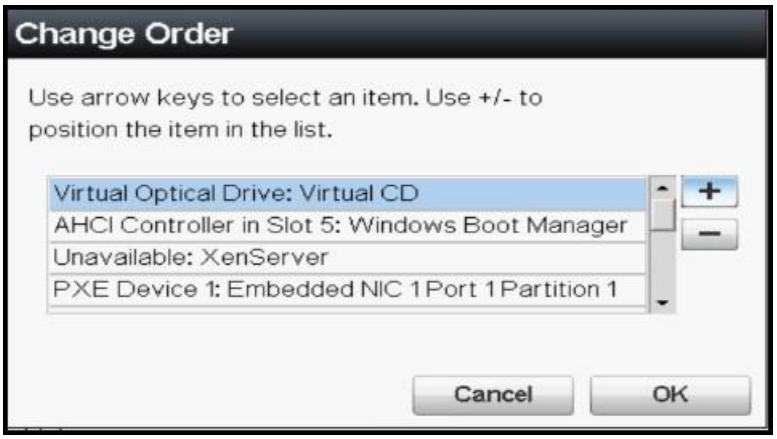


ภาพประกอบ 9 การตั้งค่าการบูต

6. คลิก UEFI Boot Settings แล้วคลิก UEFI Boot Sequence

ภาพประกอบ 10 BIOS ระบบ การตั้งค่าการบูต UEFI

7. ในหน้าต่าง Change Order ตรวจสอบให้แน่ใจว่าได้เลือก Virtual Optical Drive: Virtual CD เป็นอุปกรณ์สำหรับบูตแล้ว จากนั้นคลิก OK



ภาพประกอบ 11 หน้าจอเลือกลำดับการบูต

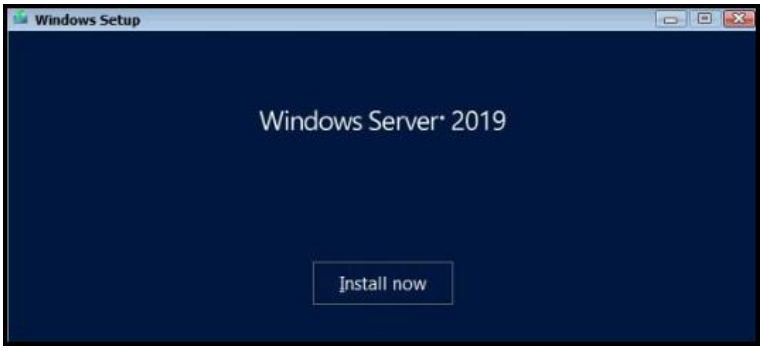
8. คลิก ย้อนกลับ
9. คลิก เสร็จสิ้น แล้วคลิก ใช่
10.คลิก เสร็จสิ้น เพื่อออกจากหน้า การตั้งค่าระบบ แล้วคลิก ใช่ เพื่อรีบูตระบบ
11.ใส่แผ่นระบบปฏิบัติการ Microsoft Windows Server 2019 ลงในไดรฟ์ DVD/CD
12.หลังจาก files ถูกโหลด เลือกภาษาที่ต้องการติดตั้งระบบปฏิบัติการ

ภาพประกอบ 12 เลือกภาษา การตั้งค่าการบูต

13.เลือกรูปแบบ ภาษา เวลา และสกุลเงิน แป้นพิมพ์ หรือวิธีการป้อนข้อมูล แล้วคลิก ถัดไป

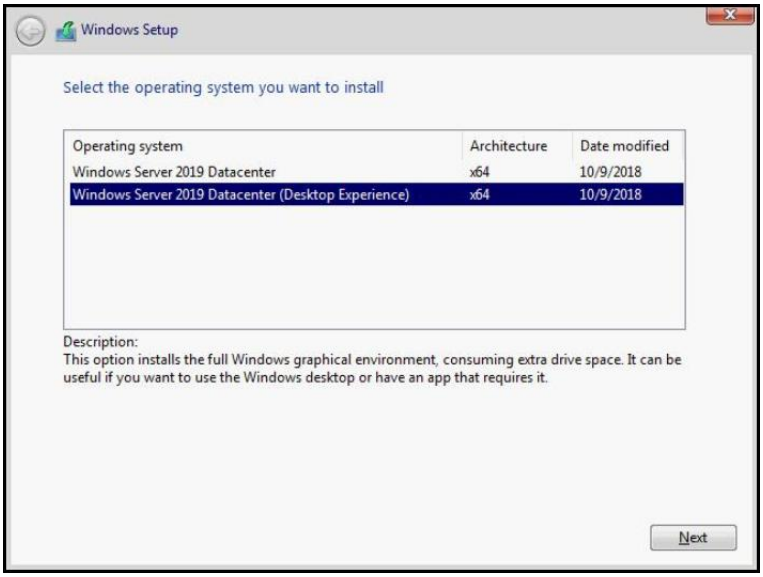
ภาพประกอบ 13 หน้าจอเลือกรูปแบบ ภาษา เวลา และสกุลเงิน แป้นพิมพ์

14.คลิก Install now



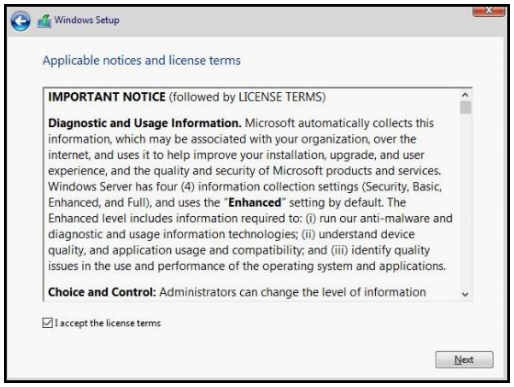
ภาพประกอบ 14 หน้าจอติดตั้งระบบปฏิบัติการ

15.เลือกระบบปฏิบัติการที่ต้องการ จากนั้นคลิก Next



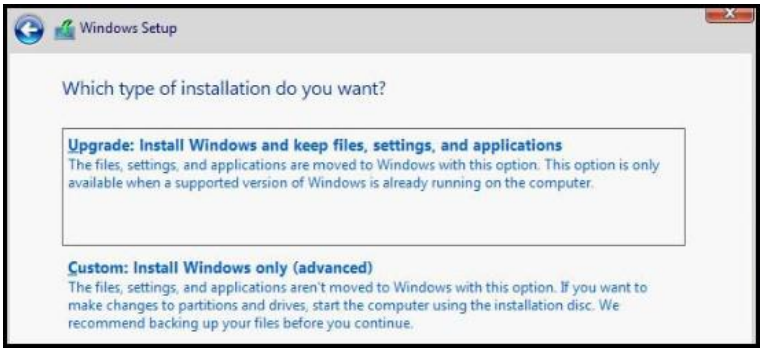
ภาพประกอบ 15 เลือกที่ต้องการติดตั้ง ระบบปฏิบัติการ

16.อ่านข้อมูลข้อตกลงสิทธิ์การใช้งาน เลือกกล่องกาเครื่องหมายถูกในช่อง I accept the license terms ถ้ายอมรับเงื่อนไขการอนุญาตให้ใช้สิทธิ์ ให้คลิก Next



ภาพประกอบ 16 ประกาศที่เกี่ยวข้องและเงื่อนไขการอนุญาตให้ใช้สิทธิ์

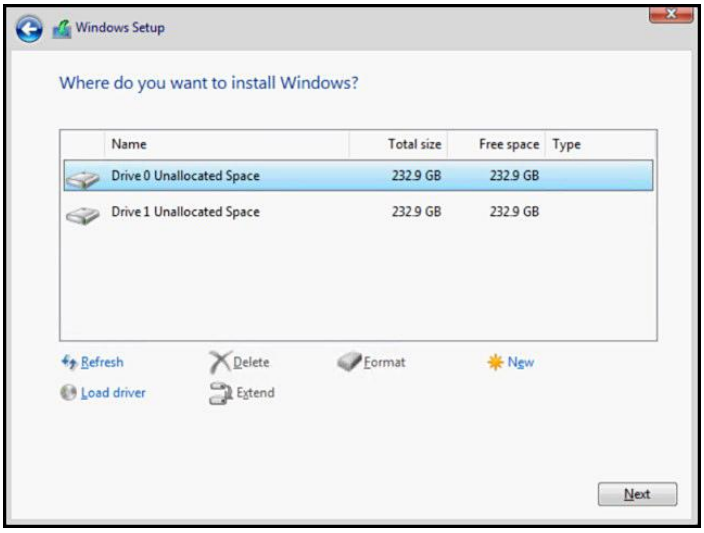
ในหน้าต่างที่ให้เลือกประเภทติดตั้งชนิดให้เลือก Custom: Install Windows only (advanced)



ภาพประกอบ 17 หน้าจอเลือกประเภทของการติดตั้ง

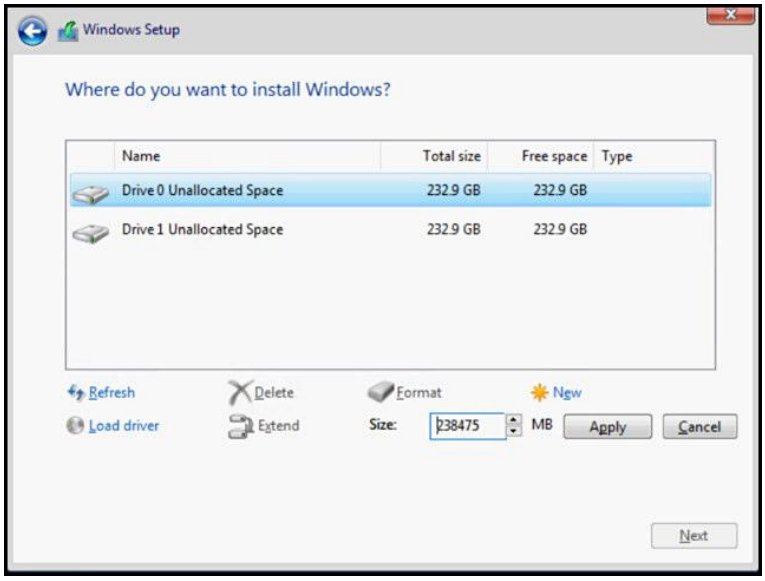
1. ให้เลือกพื้นที่ต้องการติดตั้งระบบปฏิบัติการและคลิก ที่ New เพื่อสร้างพาร์ติชันใหม่

   1) คลิก ที่ New เพื่อสร้างพาร์ติชันใหม่



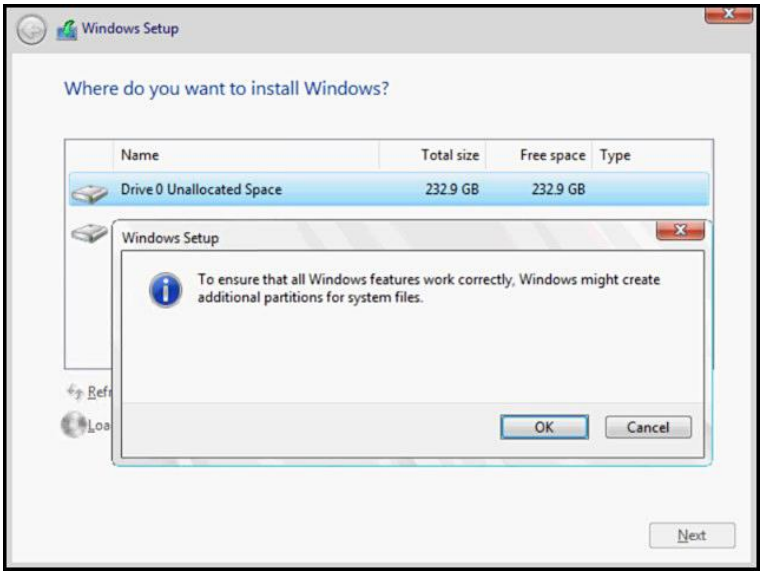
ภาพประกอบ 18 เลือกตำแหน่งที่จะติดตั้ง

2) ในกล่อง Size ให้ใส่หรือเลือกขนาดของพาร์ติชันเป็น MB แล้วคลิก Apply



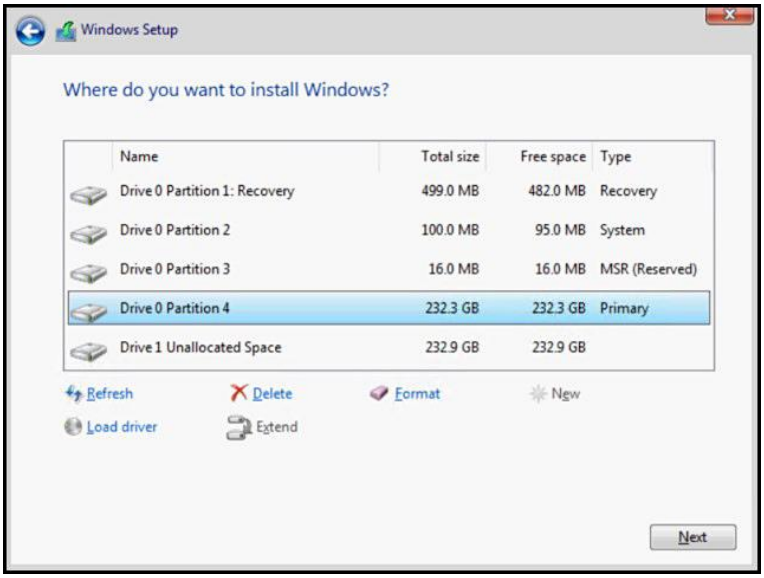
ภาพประกอบ 19 หน้าจอตั้งค่าขนาดของพาร์ติชัน

หมายเหตุ: ขนาดพาร์ติชันขั้นต่ำที่แนะนำของพาร์ติชันหลักสำหรับ Standard และ Datacenter Edition คือ 40 GB และสำหรับ Essentials Edition คือ 60 GB หากติดตั้งโมดูลหน่วยความจำเพิ่มเติมในระบบ อาจต้องใช้พื้นที่พาร์ติชันหลักเพิ่มเติมเพื่อรองรับ Page file (ไฟล์หน่วยความจำเสมือน) และ Hibernation file (ไฟล์พักข้อมูล) Hibernation file หรือชื่อไฟล์ในระบบคือ hiberfil.sys เป็นไฟล์สำคัญที่ระบบปฏิบัติการ Windows ใช้สำหรับ เก็บข้อมูลจากหน่วยความจำหลัก (RAM) ลงในพื้นที่เก็บข้อมูล (Storage) ขณะที่เข้าสู่โหมด Hibernate บทบาทของ Hibernation file:เมื่อผู้ใช้เลือก "Hibernate" แทนการ Shutdown หรือ Sleep ระบบจะบันทึกสถานะของ หน่วยความจำ (RAM) ทั้งหมด เช่น โปรแกรมที่เปิดอยู่ ไฟล์ที่กำลังทำงาน การตั้งค่าระบบ ฯลฯ ลงใน hiberfil.sys หลังจากนั้นเครื่องจะ ปิดพลังงานทั้งหมด (เหมือน Shutdown) เมื่อเครื่องทำงานอีกครั้ง Windows จะโหลดข้อมูลจาก hiberfil.sys กลับเข้าสู่ RAM กลับมาทำงานต่อจากจุดเดิมได้ทันทีระหว่างการติดตั้ง ขนาดพาร์ติชันที่แนะนำจะแสดงบนหน้าจอตามขนาดหน่วยความจำของระบบ



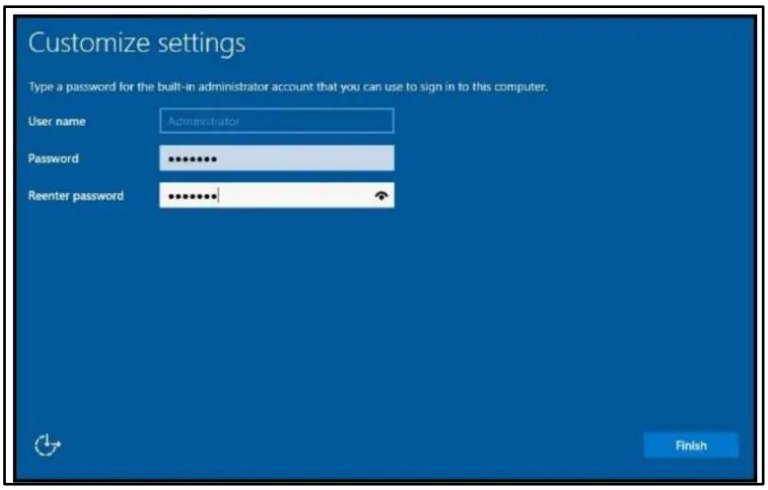
ภาพประกอบ 20 หน้าจอแจ้งเตือนอาจสร้างพาร์ติชันเพิ่มเติมสำหรับไฟล์ระบบ

2. เลือกพาร์ติชันระบบปฏิบัติการที่สร้างขึ้นใหม่ แล้วคลิก Next ระบบจะรีบูตหลังจากติดตั้งระบบปฏิบัติการแล้วเสร็จ



ภาพประกอบ 21 เลือกพาร์ติชันระบบปฏิบัติการที่สร้างขึ้นใหม่

3. ป้อนรหัสผ่านผู้ดูแลระบบ แล้วใส่อีกครั้งเพื่อยืนยันรหัสผ่าน จากนั้นคลิก **Finish**



ภาพประกอบ 22 ปรับแต่งการตั้งค่า

4. หลังจากรีบูตระบบแล้ว ให้กด Ctrl+Alt+Delete เพื่อเข้าสู่ระบบ
5. พิมพ์รหัสผ่านผู้ดูแลระบบ แล้วกด Enter เป็นอันเสร็จสิ้นขั้นตอนการติดตั้ง

การติดตั้งแม่ข่ายให้บริการเว็ปไซต์ (Web Server)

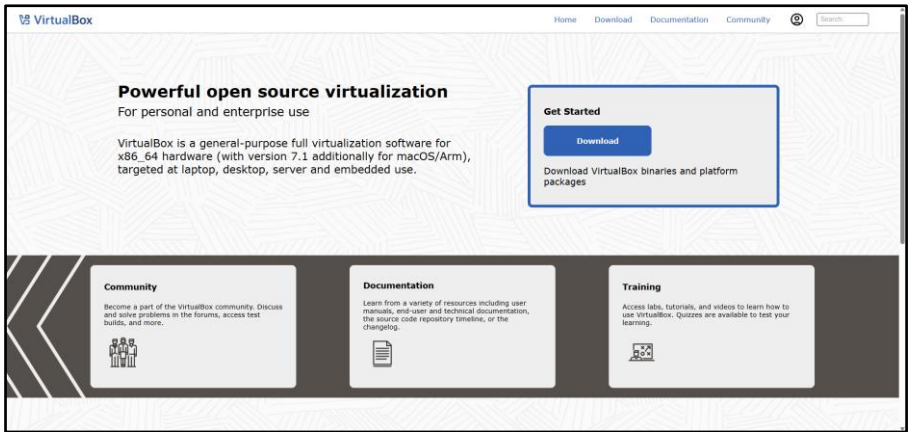
ในการให้บริการเว็ปไซต์หรือ Webserver ของสำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร นั้นใช้รูปแบบการให้บริการ 2 รูปแบบ คือ

1. Web Server ที่ติดตั้งในเครื่องคอมพิวเตอร์เสมือน หรือ Virtual Machine ใช้งานผ่านโปรแกรม Oracle VirtualBox โดยเครื่องนี้จะติดตั้งระบบปฏิบัติการ Windows Server 2008 R2 ซึ่งจะเป็นระบบเดิมที่ยังใช้งานอยู่ เช่น ระบบบริหารการศึกษา SNRU Connect ระบบบริหารจัดการหลักสูตรตามมาตรฐาน มคอ.

2. Apache Web Server เพื่อประมวลผลภาษา php เป็นหลัก เป็นระบบที่พัฒนาใหม่หรือพัฒนาเพื่อทดแทนระบบเดิมที่ไม่สามารถทำงานได้อย่างเต็มประสิทธิภาพ

ขั้นตอนที่ 1: ดาวน์โหลด Oracle VirtualBox

1. เปิดเว็บเบราว์เซอร์และไปที่เว็บไซต์ทางการของ Oracle VirtualBox: https://www.virtualbox.org



ภาพประกอบ 23 เว็บไซต์ทางการของ Oracle VirtualBox

2. คลิกที่ปุ่ม “Download VirtualBox”

3. เลือกเวอร์ชันสำหรับ Windows โดยคลิกที่ “Windows hosts”

ภาพประกอบ 24 หน้าจอเวอร์ชั่นสำหรับสำหรับดาวน์โหลด

ขั้นตอนที่ 2: ติดตั้งโปรแกรม VirtualBox

1. ดับเบิลคลิกที่ไฟล์ .exe ที่ดาวน์โหลดมา
2. คลิก Next ในหน้าต่างเริ่มต้นการติดตั้ง
3. ปรับแต่งการติดตั้งหากต้องการ หรือคลิก Next ต่อไป
4. คลิก Yes หากระบบแจ้งเตือนเรื่อง Network Interfaces
5. คลิก Install เพื่อเริ่มติดตั้ง
6. คลิก Install หากระบบแจ้งเตือนให้ติดตั้งไดรเวอร์
7. เมื่อติดตั้งเสร็จ คลิก Finish

ขั้นตอนที่ 3: ติดตั้ง Extension Pack

1. กลับไปที่หน้า https://www.virtualbox.org/wiki/Downloads
2. ดาวน์โหลด VirtualBox Extension Pack
3. ดับเบิลคลิกที่ไฟล์ .vbox-extpack
4. คลิก Install และยอมรับข้อตกลงการใช้งาน
5. คลิก OK เมื่อการติดตั้งเสร็จสิ้น

1.การติดตั้ง Web Server ที่ติดตั้งในเครื่องคอมพิวเตอร์เสมือน เพื่อเปิดระบบ SNRU Connect

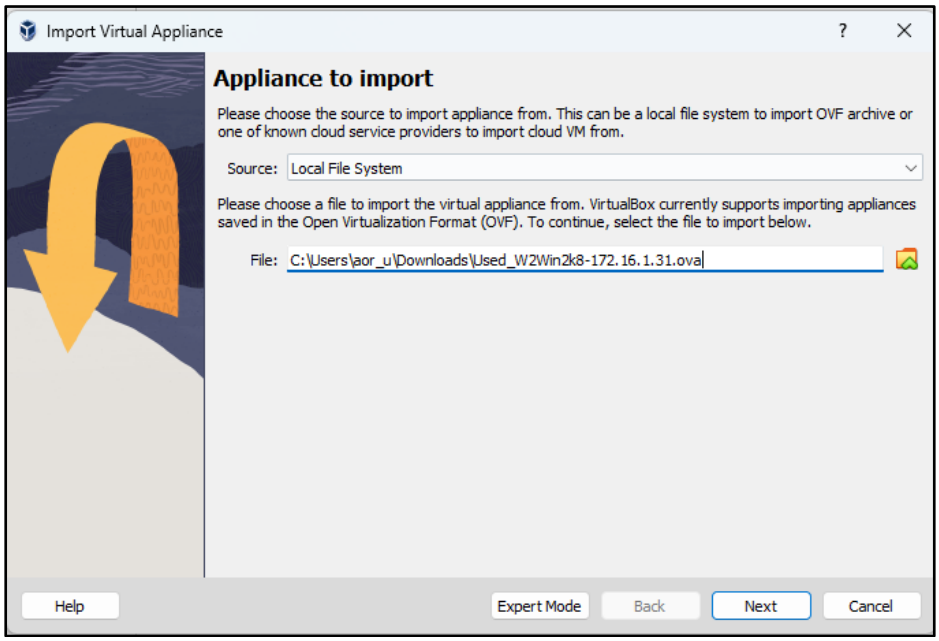
1. เปิดโปรแกรม

ภาพประกอบ 23 หน้าจอโปรแกรม Virtual Box

2. คลิกที่ Files > Import Appliance

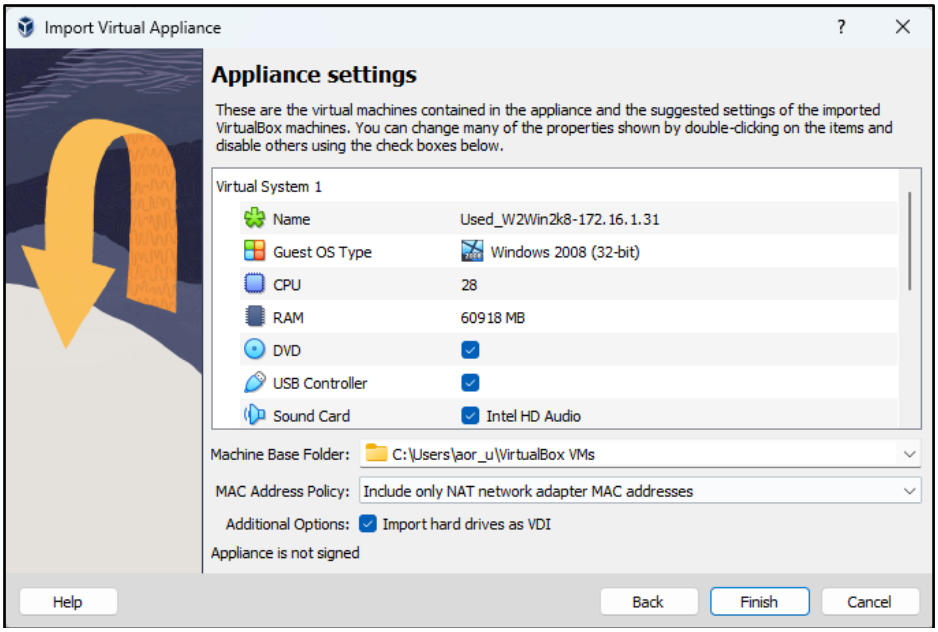
ภาพประกอบ 24 หน้าจอสำหรับนำเข้าไฟล์ .ova ที่สำรองไว้

3.เลือกไฟล์ที่เราได้สำรองไว้ แล้วคลิก Next



ภาพประกอบ 25 หน้าจอสำหรับการเลือกไฟล์

4.คลิก Finish เพื่อเริ่มกระบวนการนำเข้าระบบปฏิบัติการและโปรแกรมที่สำรองไว้

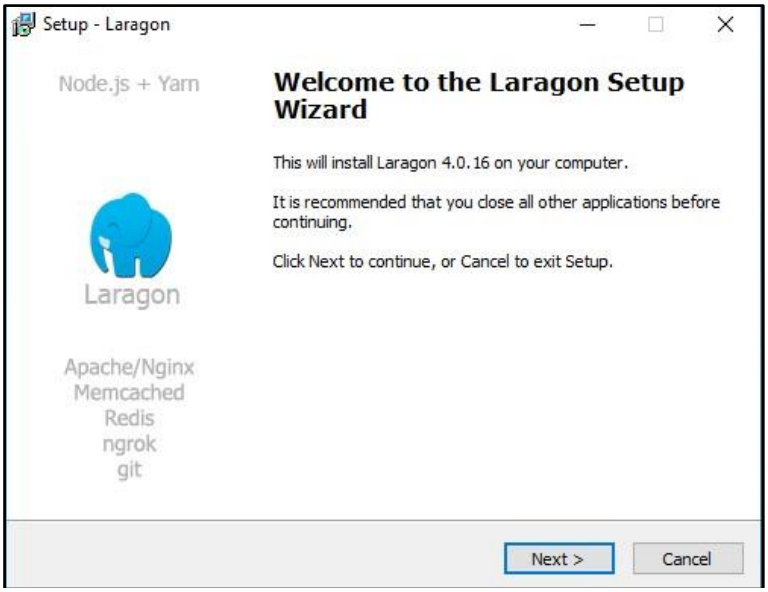


ภาพประกอบ 26 หน้าจอสำหรับการเลือกไฟล์

2. ขั้นตอนการติดตั้ง Apache Web Server ด้วย Laragon

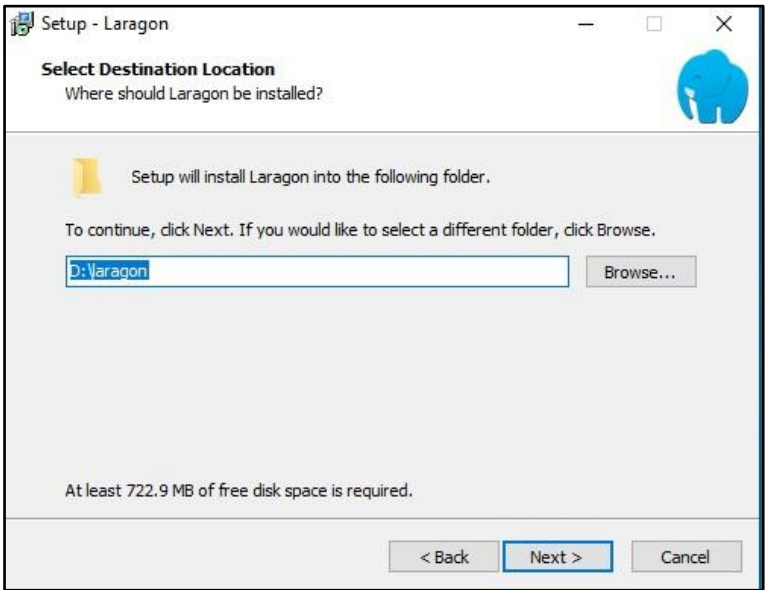
Laragon เป็นโปรแกรมจำลองที่ให้ทำหน้าที่เป็น Web Server Laragon ทำงานได้อย่างรวดเร็วและมีประสิทธิภาพสำหรับ PHP, Node.js, Python, Java, Go, Ruby รวดเร็วน้ำหนักเบาใช้งานง่ายและง่ายต่อการพัฒนา

1) เข้าไปที่ลิงก์ https://laragon.org/download/ แล้วคลิกดาวโหลดเวอร์ชั่นล่าสุด แล้วดับเบิ้ลไฟล์ที่ดาวโหลดมาแล้ว เพื่อติดตั้ง



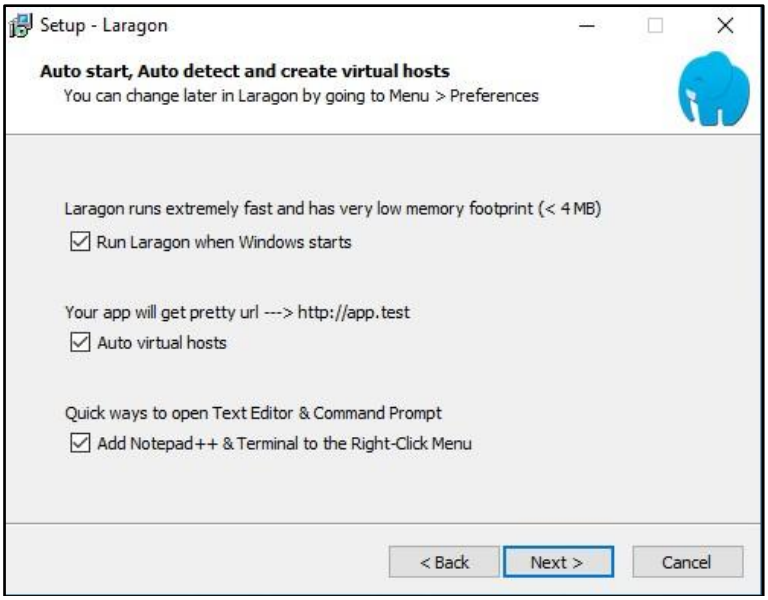
ภาพประกอบ 27 หน้าจอเริ่มต้นการติดตั้ง

2) เลือกตำแหน่งจัดเก็บที่ติดตั้งตามต้องการ แล้วคลิก Next



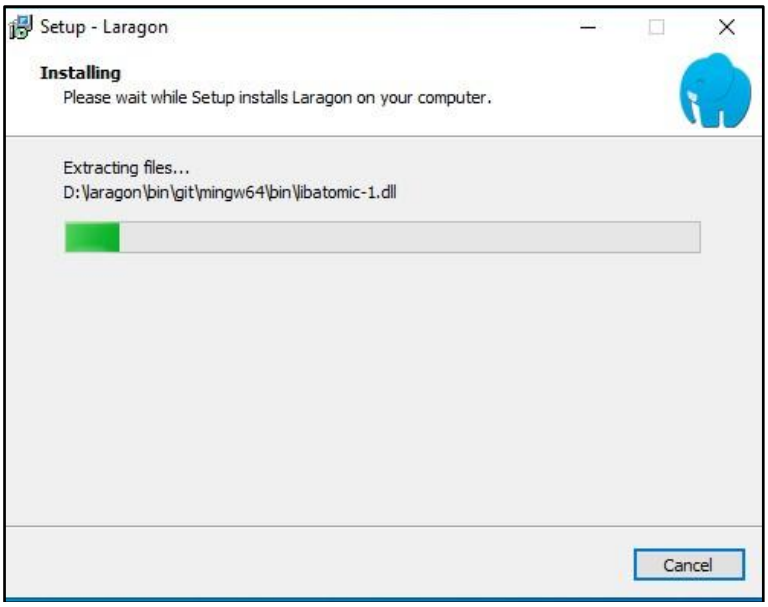
ภาพประกอบ 28 หน้าจอเลือกตำแหน่งจัดเก็บไฟล์

3) คลิก Next เพื่อเริ่มกระบวนการติดตั้งโปรแกรม



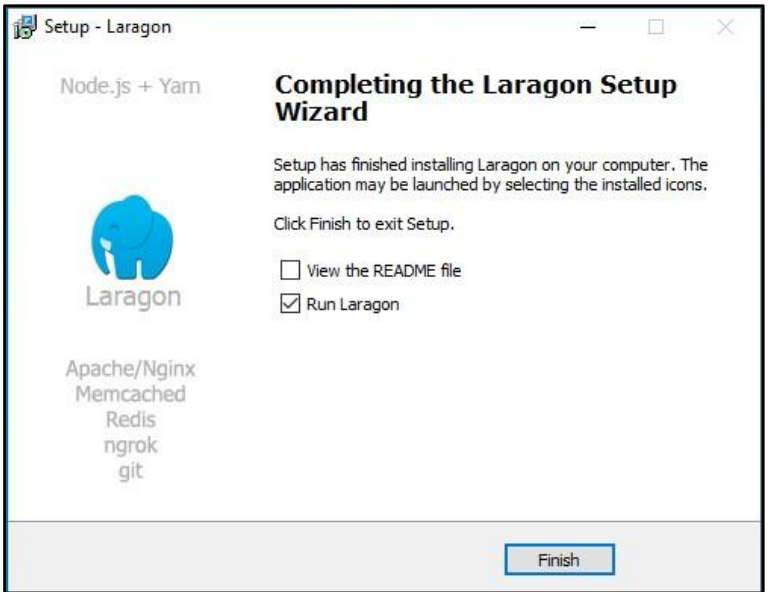
ภาพประกอบ 29 หน้าจอตั้งค่าก่อนติดตั้งโปรแกรม

4) เมื่อเริ่มกระบวนการติดตั้งโปรแกรม รอให้ระบบคัดลอกไฟล์ให้เรียบร้อย



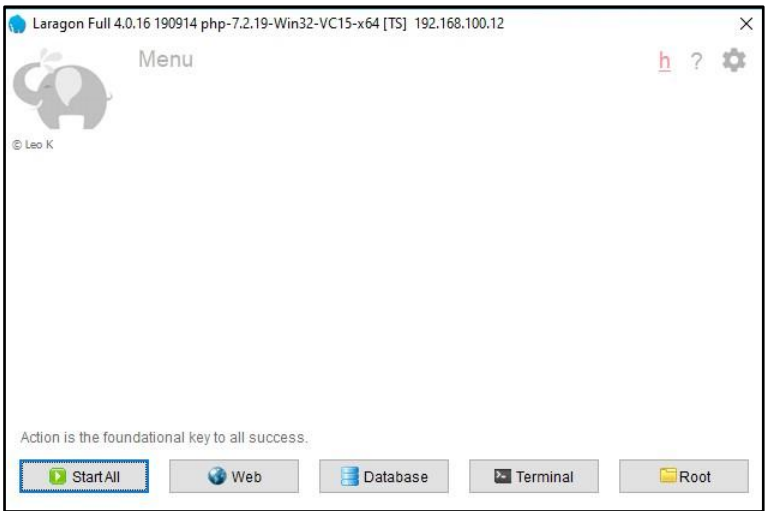
ภาพประกอบ 30 หน้าจอแสดงการแยกไฟล์ เพื่อติดตั้ง

5) เมื่อติดตั้งโปรแกรมเรียบร้อยแล้ว คลิก Finish เพื่อเริ่มต้นการทำงานของโปรแกรม



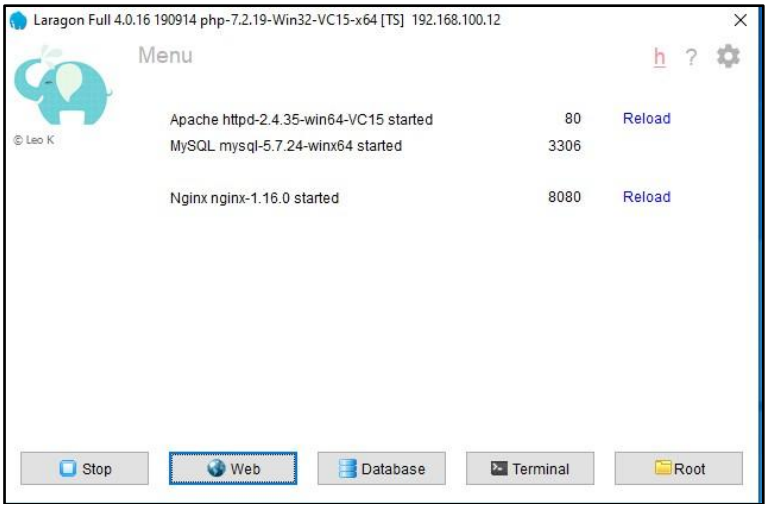
ภาพประกอบ 31 หน้าจอรายงานผลการติดตั้งโปรแกรม

6) เมื่อคลิก Finish แล้วจะปรากฏหน้าจอเพื่อเริ่มต้นการทำงานของโปรแกรมที่เกี่ยวของให้คลิกที่ Start All แล้วโปรแกรมจะเริ่มทำงาน



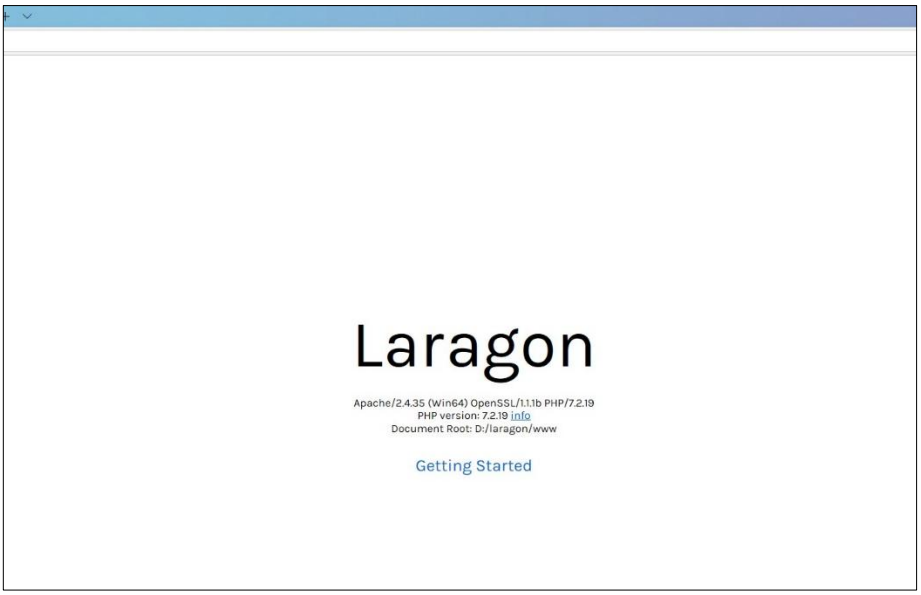
ภาพประกอบ 32 หน้าเพื่อเริ่มต้นทำงานของโปรแกรม

7) หลังจากที่คลิก Start All แล้วโปรแกรมจะแสดงสถานการณ์ทำงานของระบบจะแสดงสถานการณ์ทำงาน และพอร์ตที่เกี่ยวข้องทั้งหมด



ภาพประกอบ 33 หน้าจอแสดงสถานการณ์ทำงานของระบบ

8) หากต้องการทดสอบการทำงานของระบบสามารถเปิดบราวเซอร์และระบุไอพีแอดเดรส 127.0.0.1 หรือระบุ http://localhost ก็ได้



ภาพประกอบ 34 หน้าแรกของเว็บ

Apache Web Server คืออะไร

Apache HTTP Server (หรือเรียกสั้น ๆ ว่า Apache) คือซอฟต์แวร์ Web Server แบบ Open Source ที่ใช้รันเว็บไซต์และแอปพลิเคชันบนเว็บ ใช้กันอย่างแพร่หลายบน Linux, Windows, macOS ฯลฯ รองรับการใช้งาน PHP, Python, Perl ฯลฯ

จุดเด่นของ Apache

- รองรับโมดูล (Modules) ต่าง ๆ เช่น mod_rewrite, mod_ssl
- ตั้งค่า .htaccess ได้อย่างยืดหยุ่น
- ใช้คู่กับ PHP และ MySQL ได้อย่างดี
- เสถียร และได้รับการอัปเดตสม่ำเสมอ
- ใช้งานใน Production Server ทั่วโลก

ทำไมถึงเลือกใช้ Laragon?

Laragon เป็นชุดพัฒนาเว็บเซิร์ฟเวอร์แบบ All-in-One สำหรับ Windows โดยมาพร้อมกับ Apache, PHP, MySQL, Node.js, Composer ฯลฯ

ข้อดีของ Laragon

1. ติดตั้งง่ายมาก — ไม่ต้องเซ็ตค่าระบบเยอะ เหมาะกับผู้เริ่มต้น
2. เริ่มต้นเร็ว — เบาเครื่องกว่า XAMPP, WAMP
3. มี Auto Virtual Host — เปิดเว็บด้วยชื่อเช่น myproject.test โดยไม่ต้องแก้ hosts หรือ httpd-vhosts.conf เอง
4. สลับเวอร์ชั่น PHP ได้ง่าย — ใช้ PHP หลายเวอร์ชั่นบนเครื่องเดียว
5. เสถียรและเร็วกว่า XAMPP/WAMP ในการพัฒนา

ทำไมถึงไม่เลือก XAMPP หรือ WAMP?

คุณสมบัติ	XAMPP/WAMP	Laragon
ขนาดไฟล์ติดตั้ง	ใหญ่	เล็ก
ความเร็วในการเริ่ม	ช้า	เร็ว
สลับ PHP ได้ไหม	ยาก	ง่าย
Auto Virtual Host	ไม่มี	มี
การจัดการบริการ (Service)	ปานกลาง	ง่ายและเบา
การติดตั้ง/ถอนการติดตั้ง	ยุ่งยาก	ไม่ทิ้งไฟล์ในระบบ

ตารางเปรียบเทียบคุณสมบัติ ของXAMPP และ Laragon

ความปลอดภัยของ Apache + Laragon

ความปลอดภัยมีระดับ “ดี” ถ้า:

- ใช้ **Laragon เฉพาะในเครื่องส่วนตัว/เครื่องพัฒนา (Development)** เท่านั้น
- ปิดพอร์ตเมื่อไม่ใช้งาน (เช่น Port 80, 443)
- ไม่เปิด Laragon ให้เข้าถึงจากเครือข่ายภายนอก (Localhost เท่านั้น)
- ไม่เก็บข้อมูลสำคัญ เช่น Password จริง หรือ Database ลูกค้าในเครื่องที่ใช้ Laragon

ไม่แนะนำ:

- ใช้ Laragon เป็น **Production Server**
- เปิด Public IP หรือให้คนอื่นเข้าผ่านอินเทอร์เน็ต

หากใช้ใน **Production** ควรติดตั้ง Apache, PHP, MySQL แบบ Manual และตั้งค่าความปลอดภัยเอง (เช่น เปิด HTTPS, ตั้ง Firewall, จำกัด IP Access ฯลฯ)

สรุป

ประเด็น	คำอธิบาย
ทำไมใช้ Laragon	ใช้งานง่าย, เร็ว, มีฟีเจอร์ครบสำหรับนักพัฒนา
เทียบกับตัวอื่น	เบากว่า เสถียรกว่า XAMPP/WAMP
ความปลอดภัย	ปลอดภัยพอสมควร ถ้าใช้แค่ใน Localhost และไม่เปิดให้คนนอก
เหมาะกับ	นักพัฒนา, นักเรียน, นักศึกษาที่ฝึกทำเว็บไซต์

1. การติดตามการประเมินผลการปฏิบัติงาน

ในการติดตามสถานะการทำงานของเครื่องแม่ข่ายจำเป็นที่จะต้องมีเครื่องมือเพื่อตรวจสอบการให้บริการได้อย่างต่อเนื่อง Uptime Kuma เป็นเครื่องมือติดตามสถานะการทำงานแบบเปิดเผยรหัส (Opensource) https://github.com/louislam/uptime-kuma/ ที่ช่วยแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบปัญหาการทำงานของเครื่องแม่ข่าย

วิธีการติดตั้ง Uptime Kuma บนระบบปฏิบัติการ Windows

Uptime Kuma เป็นเครื่องมือตรวจสอบการทำงานของเซิร์ฟเวอร์และบริการแบบโอเพนซอร์ส ที่มีหน้าเว็บที่ใช้งานง่าย สามารถตรวจสอบสถานะเว็บไซต์และบริการอื่นๆ ได้อย่างมีประสิทธิภาพ เอกสารนี้จะแนะนำวิธีการติดตั้ง Uptime Kuma บนระบบปฏิบัติการ Windows

สิ่งที่จำเป็นต้องมีก่อนการติดตั้ง

1. เครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows
2. การเชื่อมต่ออินเทอร์เน็ต
3. สิทธิ์ผู้ดูแลระบบ (Administrator)

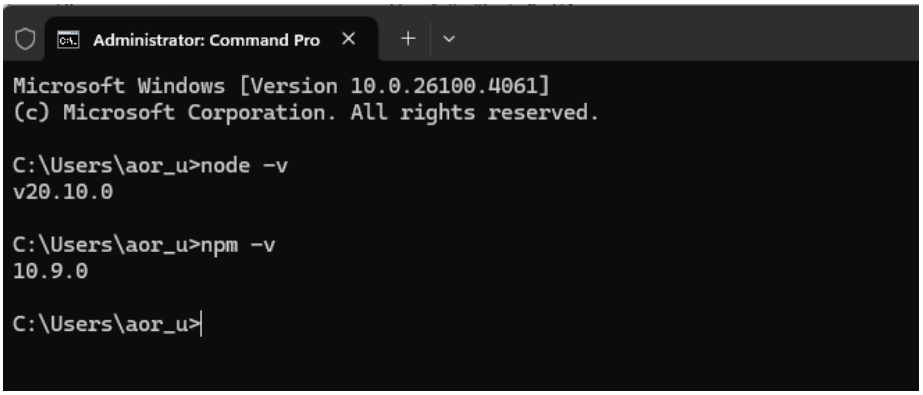
ขั้นตอนที่ 1: ติดตั้ง Node.js

Node.js เป็นสภาพแวดล้อมการทำงานที่จำเป็นสำหรับการรัน Uptime Kuma

1. ดาวน์โหลด Node.js เวอร์ชันล่าสุด (LTS) จากเว็บไซต์ทางการ: https://nodejs.org/
2. เปิดไฟล์ติดตั้งและทำตามขั้นตอนการติดตั้ง
3. ตรวจสอบให้แน่ใจว่าได้เลือกตัวเลือก "Add to PATH" เพื่อให้สามารถเรียกใช้ Node.js ได้จากทุกตำแหน่งใน Command Prompt
4. ตรวจสอบการติดตั้งโดยเปิด Command Prompt และพิมพ์คำสั่งต่อไปนี้:

```
Bash
node -v
npm -v
```

หากการติดตั้งสำเร็จ คำสั่งเหล่านี้จะแสดงเวอร์ชั่นของ Node.js และ npm ที่ติดตั้ง



ขั้นตอนที่ 2: ติดตั้ง Git

Git เป็นระบบควบคุมเวอร์ชันที่จำเป็นสำหรับการดาวน์โหลด Uptime Kuma จาก GitHub

1. ดาวน์โหลด Git สำหรับ Windows จาก: https://git-scm.com/download/win
2. เปิดตัวติดตั้งและทำตามขั้นตอน (สามารถใช้ค่าเริ่มต้นได้สำหรับผู้ใช้ทั่วไป)
3. หลังจากติดตั้งเสร็จ ตรวจสอบการติดตั้งโดยเปิด Command Prompt และพิมพ์:

```bash
git --version
```

หากการติดตั้งสำเร็จ คำสั่งนี้จะแสดงเวอร์ชันของ Git ที่ติดตั้ง

ขั้นตอนที่ 3: ดาวน์โหลดและติดตั้ง Uptime Kuma

1. เปิด Command Prompt (CMD) หรือ PowerShell ในฐานะผู้ดูแลระบบ โดยคลิกขวาที่ไอคอนและเลือก "Run as administrator"
2. เลือกตำแหน่งที่ต้องการติดตั้ง Uptime Kuma เช่น:

```bash
cd C:\
mkdir UptimeKuma
cd UptimeKuma
```

3. คัดลอก (Clone) โค้ดของ Uptime Kuma จาก GitHub:

```
Bash
  git clone https://github.com/louislam/uptime-kuma.git .
```

หมายเหตุ: เครื่องหมาย "." ท้ายคำสั่งหมายถึงให้คัดลอกไฟล์ไปยังโฟลเดอร์ปัจจุบัน

4. ติดตั้งความต้องการพื้นฐานของ Uptime Kuma:

```
Bash
  npm run setup
```

ขั้นตอนนี้อาจใช้เวลาสักครู่ เนื่องจากต้องดาวน์โหลดและติดตั้งแพ็คเกจต่างๆ

5. เริ่มต้นใช้งาน Uptime Kuma:

```
  npm start
```

เมื่อเห็นข้อความ "Listening on port: 3001" แสดงว่า Uptime Kuma ทำงานเรียบร้อยแล้ว

ขั้นตอนที่ 4: เข้าใช้งาน Uptime Kuma

1. เปิดเว็บเบราว์เซอร์ (เช่น Chrome, Firefox, Edge) และไปที่ URL:

http://localhost:3001

2. ในการใช้งานครั้งแรก คุณจะต้องสร้างบัญชีผู้ดูแลระบบ กรอกข้อมูลต่อไปนี้:
    - ชื่อผู้ใช้
    - รหัสผ่าน
    - ยืนยันรหัสผ่าน
3. หลังจากลงชื่อเข้าใช้ คุณจะเข้าสู่หน้าควบคุมของ Uptime Kuma ซึ่งคุณสามารถเริ่มตั้งค่าการตรวจสอบบริการต่างๆ ได้

การตั้งค่าให้ Uptime Kuma ทำงานเมื่อเริ่มต้น Windows

หากต้องการให้ Uptime Kuma ทำงานอัตโนมัติทุกครั้งที่เริ่มต้น Windows สามารถใช้ PM2 ซึ่งเป็นตัวจัดการกระบวนการสำหรับ Node.js:

1.ติดตั้ง PM2 ผ่าน npm:

```
npm install -g pm2
```

2.ตั้งค่าให้ Uptime Kuma ทำงานผ่าน PM2:

```
pm2 start server/server.js --name uptime-kuma
```

3. บันทึกการตั้งค่า PM2:

```
pm2 save
```

4. ตั้งค่าให้ PM2 ทำงานเมื่อเริ่มต้น Windows:

```
npm install -g pm2-windows-startup
pm2-startup install
```

หลังจากนี้ Uptime Kuma จะทำงานอัตโนมัติทุกครั้งที่เริ่มต้น Windows และสามารถเข้าถึงได้ที่ http://localhost:3001

ภาพประกอบ 34 หน้าจอแสดงติดตามการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย

บทที่ 5

สรุปและข้อเสนอแนะ

ผู้ปฏิบัติงานตามคู่มือการปฏิบัติงาน เรื่อง การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร ในบทบาทหน้าที่ของผู้ปฏิบัติงานนั้นมี กฎระเบียบ หลักเกณฑ์ และ ทฤษฎีที่เกี่ยวข้องและต้องปฏิบัติให้เป็นไปตามนั้นอยู่หลายส่วนด้วยกัน นอกจากผู้ปฏิบัติงานจะต้องเป็นผู้รอบรู้ใน กฎระเบียบ ทฤษฎีที่เกี่ยวข้องและปฏิบัติได้เป็นอย่างดีแล้ว ยังต้องทำหน้าที่ในการให้ทำปรึกษาแนะนำแก่ผู้รับบริการ อีกด้วย และยังต้องมีส่วนร่วมในการร่วมแก้ไขปัญหาเกี่ยวกับการปฏิบัติงาน ซึ่งสามารถสรุปประเด็นปัญหาอุปสรรคได้ดังต่อไปนี้

การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) มีขั้นตอนหลักดังนี้

1) เตรียมฮาร์ดแวร์

- เตรียมตัวเครื่องคอมพิวเตอร์แม่ข่ายที่มีสเปกเหมาะสม เช่น CPU, RAM, HDD/SSD ที่เพียงพอ
- จัดเตรียมอุปกรณ์ต่อพ่วง เช่น จอภาพ, คีย์บอร์ด, เมาส์ (ถ้ามี)

2) ติดตั้งระบบปฏิบัติการสำหรับเซิร์ฟเวอร์

- ใส่แผ่นดิสก์หรือบูตจาก USB ของระบบปฏิบัติการสำหรับเซิร์ฟเวอร์ เช่น Windows Server, Linux (Ubuntu Server, CentOS เป็นต้น)
- ปฏิบัติตามขั้นตอนการติดตั้งจากหน้าจอ

3) กำหนดค่าพื้นฐานของระบบ

- ตั้งค่ารหัสผ่านผู้ดูแลระบบ (root หรือ administrator)
- กำหนดค่าเครือข่าย เช่น IP Address, Subnet Mask, Gateway
- ติดตั้งและอัปเดตไดร์เวอร์ที่จำเป็น

4) ติดตั้งซอฟต์แวร์และบริการที่จำเป็น

- ติดตั้งโปรแกรมประยุกต์ต่างๆที่ต้องการให้บริการ เช่น Web Server, Database Server, Email Server
- ติดตั้งซอฟต์แวร์สำหรับการบริหารจัดการระบบ เช่น Monitoring Tools, Backup Solutions

5) กำหนดค่าความปลอดภัย

- ติดตั้งและกำหนดค่า Firewall
- ติดตั้งและกำหนดค่าโปรแกรมป้องกันไวรัส
- จัดการสิทธิ์การเข้าถึงระบบอย่างเหมาะสม

6) การทดสอบและปรับแต่ง

- ทดสอบการทำงานของระบบและบริการต่างๆ
- ปรับแต่งการตั้งค่าเพื่อประสิทธิภาพสูงสุด

7) การบำรุงรักษา

- จัดทำแผนสำรองข้อมูล (Backup Plan)
- ติดตั้งอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ
- ตรวจสอบประสิทธิภาพและปัญหาของระบบอย่างต่อเนื่อง

การติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่ายนั้นค่อนข้างซับซ้อน ดังนั้นควรศึกษาและดำเนินการโดยผู้มีความรู้ความชำนาญในด้านนี้เป็นอย่างดี เพื่อให้ได้ระบบที่มีประสิทธิภาพและความปลอดภัยสูงสุด

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
1. การติดตั้งระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย	**1. ปัญหาฮาร์ดแวร์** - ฮาร์ดแวร์ไม่สามารถรองรับระบบปฏิบัติการที่ต้องการติดตั้งได้ - ปัญหาการรองรับชิปเซ็ต RAID หรืออุปกรณ์จัดเก็บข้อมูล - ปัญหาการตรวจพบและใช้งานอุปกรณ์ต่อพ่วงบางอย่าง **2. ปัญหาบูตและติดตั้ง** - เครื่องไม่สามารถบูตจากสื่อติดตั้งได้ - การแบ่งพาร์ติชันดิสก์ผิดพลาด - การติดตั้งหยุดกลางคันหรือขัดข้อง - ข้อผิดพลาดจากการอัปเดตไดรเวอร์ **3. ปัญหาเครือข่ายและการเข้าถึง** - การตั้งค่า IP address ผิดพลาด - ปัญหาการตั้งค่าไฟร์วอลล์หรือการสื่อสารระหว่างเครือข่าย	การเตรียมความพร้อมทั้งด้านฮาร์ดแวร์ การศึกษาเอกสารอย่างละเอียด และปฏิบัติตามขั้นตอนปฏิบัติที่ดีที่สุดจะช่วยลดความเสี่ยงในการพบปัญหาเหล่านี้ โดยหากพบปัญหา คุณอาจต้องทำการแก้ไข โดยอ้างอิงจากคู่มือหรือขอความช่วยเหลือจากผู้เชี่ยวชาญ

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
	4. ปัญหาความเข้ากันได้ - ซอฟต์แวร์บางตัวอาจไม่สามารถทำงานบนระบบปฏิบัติการนั้นได้ - ข้อผิดพลาดจากการติดตั้งโปรแกรมเสริม เช่น ไดรเวอร์ **5. ปัญหาด้านความปลอดภัย** - การกำหนดรหัสผ่านไม่ปลอดภัย - การตั้งค่าการเข้ารหัสและระบบไฟร์วอลล์ไม่ถูกต้อง - มีช่องโหว่หรือจุดอ่อนด้านความปลอดภัย **6. ปัญหาการปรับแต่งและอัปเกรด** - การอัปเดตแก้ไขอาจนำไปสู่ปัญหาความเข้ากันไม่ได้หรือข้อผิดพลาด - การปรับแต่งการตั้งค่าอาจทำให้ระบบทำงานผิดปกติ	

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
2. การสร้างคอมพิวเตอร์เสมือน Virtual Server	**1. ประสิทธิภาพการทำงาน** - การจำลองทรัพยากรอาจทำให้ประสิทธิภาพลดลงเมื่อเทียบกับคอมพิวเตอร์กายภาพ - การติดตั้งคอมพิวเตอร์เสมือนหลายเครื่องบนเครื่องกายภาพเดียวกันอาจนำไปสู่ปัญหาการขาดทรัพยากรของระบบ เช่น CPU RAM พื้นที่จัดเก็บข้อมูล **2. การจัดการทรัพยากร** - การจัดสรรทรัพยากรที่ไม่เหมาะสมอาจทำให้เกิดปัญหาประสิทธิภาพหรือความล้มเหลวของระบบ - การสำรองข้อมูลและการกู้คืนอาจซับซ้อนขึ้นเนื่องจากต้องจัดการทั้งเครื่องกายภาพและเสมือน	การป้องกันปัญหาเหล่านี้ ควรศึกษาและทำความเข้าใจในการใช้งานคอมพิวเตอร์เสมือนอย่างถูกต้อง การวางแผน การจัดสรรทรัพยากรอย่างเหมาะสม การรักษาความปลอดภัย และการทดสอบระบบอย่างสม่ำเสมอ นอกจากนี้ การปรึกษาผู้เชี่ยวชาญและศึกษาแนวปฏิบัติที่ดีที่สุดจะช่วยลดโอกาสเกิดปัญหาได้

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
	3. ความซับซ้อนในการติดตั้งและกำหนดค่า - การติดตั้งและกำหนดค่าซอฟต์แวร์เสมือนและระบบปฏิบัติการเสมือนอาจซับซ้อน - การทำให้ระบบเสมือนสามารถสื่อสารกับระบบกายภาพและเสมือนอื่นๆ ได้อาจเป็นเรื่องยาก **4. การเข้ากันไม่ได้ของซอฟต์แวร์และไดรเวอร์** - ซอฟต์แวร์หรือไดรเวอร์บางตัวอาจไม่สามารถทำงานบนสภาพแวดล้อมเสมือนได้อย่างถูกต้อง **5. ปัญหาด้านความปลอดภัย** - การเข้าถึงระบบเสมือนโดยไม่ได้รับอนุญาตอาจเกิดขึ้นได้หากไม่มีการรักษาความปลอดภัยที่เหมาะสม - การร่วมแชร์ทรัพยากรอย่างไม่ระมัดระวังอาจนำไปสู่ความเสี่ยงด้านความปลอดภัย	

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
	6. ปัญหาการสนับสนุน - เมื่อเกิดปัญหากับระบบเสมือน การแก้ไขอาจซับซ้อนกว่าระบบกายภาพ - ความเข้ากันได้ของระบบเสมือนกับระบบจริงอาจมีข้อจำกัด	
3. การติดตั้งดาต้าเบสเซิร์ฟเวอร์ระบบงานทะเบียนนักศึกษา	**1. ปัญหาด้านฮาร์ดแวร์** - ทรัพยากรฮาร์ดแวร์ไม่เพียงพอ เช่น CPU, RAM, พื้นที่จัดเก็บข้อมูลไม่เพียงพอ - ปัญหาความเข้ากันได้ระหว่างฮาร์ดแวร์และซอฟต์แวร์ฐานข้อมูล **2. ปัญหาการเข้าถึงและสิทธิ์** - ปัญหาการกำหนดสิทธิ์ผู้ใช้งาน ผู้ดูแลระบบที่ไม่ถูกต้อง - การตั้งค่าการเข้าถึงฐานข้อมูลจากระยะไกลไม่ถูกต้อง - การเปิดพอร์ตบนไฟร์วอลล์สำหรับฐานข้อมูลไม่ถูกต้อง	

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
	3. ปัญหาระหว่างขั้นตอนการติดตั้ง อาจเนื่องจากความขัดแย้งกับโปรแกรม - อื่นหรือการตั้งค่าระบบ - ปัญหาการตั้งค่าพารามิเตอร์ต่างๆ ระหว่างการติดตั้งไม่ถูกต้อง **4. ปัญหาการกำหนดค่าฐานข้อมูล** - การสร้างฐานข้อมูล การกำหนดค่าการเข้ารหัส การสำรองข้อมูลไม่ถูกต้อง - ปัญหาการเชื่อมต่อกับฐานข้อมูล การตรวจสอบสิทธิ์ผู้ใช้ **5. ปัญหาการทำงานร่วมกับระบบอื่นๆ** - ปัญหาการทำงานร่วมกับแอพพลิเคชันอื่นๆ ที่เชื่อมต่อกับฐานข้อมูล - การปรับแต่งและการเข้ากันได้ของซอฟต์แวร์ที่เกี่ยวข้องกับฐานข้อมูล	

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
	6. ปัญหาประสิทธิภาพและความปลอดภัย - การปรับแต่งประสิทธิภาพฐานข้อมูลที่ไม่ถูกต้อง - การรักษาความปลอดภัยฐานข้อมูล เช่น การเข้ารหัส การตรวจสอบสิทธิ์ที่ไม่เพียงพอ	
4.การติดตั้ง เว็บเซิร์ฟเวอร์ ด้วย Laragon	1. **ประสิทธิภาพการทำงานลดลง** - เซิร์ฟเวอร์อาจรองรับการเข้าถึงจำนวนมากไม่ไหว ทำให้เว็บไซต์ช้าหรือล่ม - หน่วยประมวลผลกลาง (CPU) และหน่วยความจำ (RAM) ถูกใช้งานจนเต็มประสิทธิภาพ - มีการเรียกข้อมูลอย่างต่อเนื่องจากเครื่องลูกข่ายที่เชื่อมต่อ ทำให้เกิดความล่าช้าในการแสดงผลข้อมูล 2. **ปัญหาด้านความปลอดภัย** - มีความเสี่ยงจากการโจมตีทางด้านความปลอดภัยมากขึ้น เช่น DDoS Attack - ช่องโหว่ด้านความปลอดภัยที่เคยมีอยู่อาจถูกแสวงหาประโยชน์มาก	การรับมือกับปัญหาเหล่านี้ ผู้พัฒนาและผู้ดูแลระบบต้องมีการวางแผน ออกแบบและปรับปรุงโครงสร้างพื้นฐาน เพื่อให้สามารถรองรับปริมาณผู้ใช้งานที่เพิ่มขึ้นได้อย่างมีประสิทธิภาพ เทคนิคต่างๆ เช่น การใช้งาน Nginx, Docker Load Balancer,Caching,Content Delivery Network (CDN) และการใช้งานระบบคลาวด์ อาจถูกนำมาประยุกต์ใช้

ขั้นตอนการปฏิบัติงาน	ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา/อุปสรรค
	ขึ้น	
	3. **การจัดการทรัพยากรที่ยากขึ้น** - ต้องมีการจัดสรรทรัพยากรเซิร์ฟเวอร์ เช่น CPU, RAM, Storage อย่างมีประสิทธิภาพ - การบริหารจัดการแคชและเซสชันให้เหมาะสมกับปริมาณผู้ใช้งาน 4. **ความต้องการในการขยายขนาด (Scalability)** - จำเป็นต้องมีการขยายขนาดของระบบ เช่น เพิ่มจำนวนเซิร์ฟเวอร์ หรือใช้เทคนิค Load Balancing - การออกแบบระบบให้สามารถรองรับการขยายขนาดได้อย่างราบรื่น 5. **ความท้าทายด้านการตรวจสอบและแก้ไขปัญหา** - การตรวจสอบและวิเคราะห์ปัญหาที่เกิดขึ้นอาจยากขึ้น เนื่องจากมีข้อมูลจำนวนมาก - การระบุจุดที่เป็นปัญหาและการแก้ไขให้ทันท่วงทีเป็นเรื่องสำคัญ	

บรรณานุกรม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560. (24 มกราคม 2560). ราชกิจจานุเบกษา เล่ม 134 ตอนที่ 10 ก หน้า 27-30.

วิกิพีเดีย สารานุกรมเสรี. (2566, 10 ธันวาคม). มัลแวร์. สืบค้นเมื่อ 20 พฤษภาคม 2567 จาก http://th.wikipedia.org/wiki/มัลแวร์.

Dell Inc. (2024). *Microsoft Windows Server 2019 for EMC PowerEdge Servers*. คู่มือการติดตั้งและการกำหนดค่า. สืบค้นจาก https://manuals.plus/th/dell/microsoft-windows-server-2019-for-emc-poweredge-servers-manual#microsoft_windows_server_2019_for_emc_poweredge_servers

louisiam. (2566). *Uptime Kuma:* เซิร์ฟเวอร์คอมพิวเตอร์. GitHub. สืบค้นจาก https://github.com/louisiam/uptime-kuma

louisiam. (2566). *คู่มือ Uptime Kuma*. GitHub. สืบค้นจาก https://github.com/louisiam/uptime-kuma/wiki

ภาคผนวก

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยราชภัฏสกลนคร
พ.ศ. ๒๕๕๗

คำนำ

ตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ดังนั้น มหาวิทยาลัยราชภัฏสกลนคร จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏสกลนคร พ.ศ. ๒๕๕๗ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯจากบุคลากรทุกคนและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยี ที่เปลี่ยนแปลงไปอย่างรวดเร็ว มหาวิทยาลัยราชภัฏสกลนคร จึงหวังเป็นอย่างยิ่งว่า นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งานผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏสกลนครทุกคน ถือปฏิบัติโดยเคร่งครัดต่อไป

สารบัญ

หน้า

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร พ.ศ. ๒๕๕๗

หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้า น สารสนเทศเพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น มหาวิทยาลัยราชภัฏสกลนคร จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด

วัตถุประสงค์

๑. เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขอ ง มหาวิทยาลัยราชภัฏกลนครเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒. เพื่อกำหนดแนวทางและวิธีการปฏิบัติสำหรับบุคลากรและบุคคลที่ปฏิบัติงานให้กับมหาวิทยาลัย ราชภัฏสกลนคร ในการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยี สารสนเทศ

๓. เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่ สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ ให้มีระบบสำรองสามารถทำงานได้ อย่างต่อเนื่องและสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๔. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและ ระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๕. เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการให้การอบรมทางด้านการ รักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร พ.ศ. ๒๕๕๗

๑. ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัยราชภัฏสกลนคร
๒. มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข ที่เหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายที่เกี่ยวข้อง
๓. เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ
๔. เผยแพร่ความรู้ ความเข้าใจด้านความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อสร้างความตระหนักให้บุคลากรของมหาวิทยาลัยราชภัฏสกลนครและบุคคลที่เกี่ยวข้อง
๕. ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร พ.ศ. ๒๕๕๗

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสกลนครจัดทำขึ้นเพื่อกำหนดวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งนโยบายออกเป็นส่วนๆ ดังต่อไปนี้

ส่วนที่ ๑. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
ส่วนที่ ๒. แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย
ส่วนที่ ๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย
ส่วนที่ ๔. แนวปฏิบัติของผู้ดูแลระบบ
ส่วนที่ ๕. แนวปฏิบัติการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน
ส่วนที่ ๖. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง
ส่วนที่ ๗. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ส่วนที่ ๘. การกำหนดผู้รับผิดชอบ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

“มหาวิทยาลัย” หมายถึง มหาวิทยาลัยราชภัฏสกลนคร

“สำนักวิทยบริการฯ” หมายถึง สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของมหาวิทยาลัยได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ความมั่นคงปลอดภัย” หมายถึง ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“ระบบแลน (Local Area Network)” และ **“ระบบอินทราเน็ต (Intranet)”** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในมหาวิทยาลัยเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในมหาวิทยาลัย

“ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของมหาวิทยาลัย เข้ากับเครือข่ายอินเทอร์เน็ตสากล

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึง ระบบงานของมหาวิทยาลัย ที่นำเอาเทคโนโลยีสารสนเทศและการสื่อสาร ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

“เครื่องคอมพิวเตอร์” หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย

“ผู้ใช้งาน” หมายถึง ผู้บริหาร คณาจารย์ บุคลากร พนักงานหรือลูกจ้างของมหาวิทยาลัย นักศึกษา รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย

“ผู้ดูแลระบบ (System Administrator)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“บุคคลภายนอก” หมายถึง บุคคลที่ไม่ได้สังกัดอยู่ในมหาวิทยาลัย แต่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของมหาวิทยาลัย โดยจะได้รับสิทธิ์ในการใช้ระบบตามหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง พื้นที่ที่มหาวิทยาลัยอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

๑) ที่ทำงาน หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลประจำโต๊ะทำงาน และคอมพิวเตอร์แบบพกพา รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือระบบเครือข่ายหมายถึงบริเวณติดตั้งเครื่องแม่ข่าย (Server) และอุปกรณ์เครือข่ายของมหาวิทยาลัย

๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายถึง พื้นที่ครอบคลุมในการให้บริการระบบเครือข่ายไร้สาย

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่ายซอฟต์แวร์ที่มีลิขสิทธิ์
เป็นต้น

“จดหมายอิเล็กทรอนิกส์ (e-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

“รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“บัญชีผู้ใช้งาน (Account)” หมายถึง รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของมหาวิทยาลัย

“เวลาอ้างอิงสากล (Stratum 0)” หมายถึง การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ข้อมูลจราจรทางคอมพิวเตอร์ (Log)” หมายถึง ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“โปรแกรมประสงค์ร้าย (Malware)” หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (ComputerVirus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง(Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

“ชื่อเครื่องคอมพิวเตอร์ (Computer Name)” หมายถึง ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย
“สื่อบันทึกพกพา” หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น
“ปุ่มกดง่าย (Shortcut)” หมายถึง เครื่องมือที่ช่วยในการเรียกใช้โปรแกรมได้อย่างรวดเร็วและสามารถเข้าถึงโปรแกรมหรือแฟ้มข้อมูลที่ต้องการได้ทันที ซึ่งผู้ใช้สามารถลบหรือสร้างใหม่ได้
“ไบออส (BIOS)” หมายถึง ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด
“การตั้งค่าระบบ (Configuration)” หมายถึง ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์
“เลขที่อยู่ไอพี (IP Address)” หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่ายซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)
“เลขที่อยู่ไอพีสาธารณะ (Public IP Address)” หมายถึง เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงานหรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้
“แบนด์วิดท์ (Bandwidth)” หมายถึง ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบเป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล
“ชื่อผู้ใช้ (Username)” หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้
“ลงบันทึกเข้า (Login)” หมายถึง กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง
“ลงบันทึกออก (Logout)” หมายถึง กระบวนการที่ผู้ใช้ งานทำเพื่อสิ้นสุดการใช้ งานระบบคอมพิวเตอร์และระบบเครือข่าย
“อัพเดท (Update)” หมายถึง ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ
“ช่องโหว่ (Vulnerability)” หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
“ไฟล์ที่สามารถประมวลผลได้ (Executable file)” หมายถึง ไฟล์โปรแกรมที่สามารถเรียกใช้ งานได้ทันที เช่น .exe .com .bat .vbs .scr .pif .hta .txt .doc .xls ในขณะที่ไฟล์ข้อมูลอื่นๆ จะเป็นไฟล์ข้อมูลประกอบ
“การเข้ารหัส (Encryption)” หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

“อุปกรณ์กระจายสัญญาณ (Access Point)” หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

“SSID (Service Set Identifier)” หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

“โดยปริยาย (Default)” หมายถึง ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้งาน

“WEP (Wired Equivalent Privacy)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

“WPA (Wi-Fi Protected Access)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

“Wireless LAN Client” หมายถึง เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE 802.11

“MAC Address (Media Access Control Address)” หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

“ไฟร์วอลล์ (Firewall)” หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

“VPN (Virtual Private Network)” หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

“Web Server” หมายถึง เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

“ชื่อโดเมนย่อย (Sub Domain Name)” หมายถึง ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้ เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ “ที่อยู่เว็บไซต์” แทนก็ได้

“อุปกรณ์จัดเส้นทาง (Router)” หมายถึง อุปกรณ์ที่ใช้ ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“อุปกรณ์กระจายสัญญาณข้อมูล (Switch)” หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

“การพิสูจน์ยืนยันตัวตน (Authentication)” หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยว ข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

“แผนผังระบบเครือข่าย (Network Diagram)” หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัย

“Command Line” หมายถึง บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

“Firewall Log” หมายถึง การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในมหาวิทยาลัย

“DOD 5220.22-M” หมายถึง การลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับและใช้ งานกับกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ ซึ่งทำการลบข้อมูล ๓ รอบรอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลไบต์สุ่ม

“ผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (Internal IT Auditor)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log)

“ผู้ตรวจสอบระบบสารสนเทศจากหน่วยงานภายนอก (External IT Auditor)” หมายถึง ผู้ที่ได้รับมอบหมายจากมหาวิทยาลัย ให้มีสิทธิในการตรวจสอบระบบสารสนเทศหรือระบบเครือข่ายของมหาวิทยาลัย

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้ งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัย” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และ ความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Information security incident)” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจไม่คาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ส่วนที่ ๑
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานที่เป็นบุคลากรของมหาวิทยาลัย และบุคคลภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

๒. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ การออกแบบอาคารหรือก่อสร้างใหม่ ให้สำนักวิทยบริการฯเป็นผู้ร่วมกำหนดพื้นที่ผู้ใช้งาน พื้นที่ใช้งาน ระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น ในกรณีที่ตัวอาคารสถานที่สร้างเสร็จแล้ว และมีการกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ผู้รับผิดชอบอาคารสถานที่ส่งมอบพิมพ์เขียวของตัวอาคารให้สำนักวิทยบริการฯ เพื่อใช้ในการวางแผนติดตั้งระบบเครือข่าย

๒.๒ ให้สำนักวิทยบริการฯเป็นผู้กำหนดสิทธิ์ ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ ให้สำนักวิทยบริการฯกำหนดมาตรการควบคุมการเข้า – ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๒
แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้งานที่เป็นบุคลากรของ มหาวิทยาลัย และบุคคลภายนอก ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่าง เคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของมหาวิทยาลัยให้เป็นความลับ มีความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑ ผู้ใช้งานจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑.๑ ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนสู่ระบบคอมพิวเตอร์

๒.๑.๒ นำข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๓ นำข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชนเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๔ นำข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญาเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๕ นำข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้เข้าสู่ระบบคอมพิวเตอร์

๒.๑.๖ นำข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย เข้าสู่ระบบคอมพิวเตอร์

๒.๑.๗ เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม ๒.๑.๑ ถึง ๒.๑.๖

๒.๒ ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม ๒.๑ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๒.๓ ผู้ใช้งานจะต้องไม่กระทำการ ดังต่อไปนี้

๒.๓.๑ เข้าใช้ระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบ

๒.๓.๒ นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ เช่น รหัสผ่าน ไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๒.๓.๓ เข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบ

๒.๓.๔ กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๒.๓.๕ ทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน โดยมิชอบ

๒.๓.๖ กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ

๒.๓.๗ ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

๒.๓.๘ กระทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจ ของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๒.๓.๙ ผู้ใช้งานจะต้องรับผิดชอบลิขสิทธิ์โปรแกรมคอมพิวเตอร์และการกระทำใดๆอันเกิดจากการใช้คอมพิวเตอร์แบบพกพา (Notebook) อันเป็นทรัพย์สินส่วนตัวของผู้ใช้งาน

๒.๓.๑๐ ห้ามมิให้ใช้ระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย เพื่อการพาณิชย์หรือการอื่นใดที่ไม่เกี่ยวข้องกับหน้าที่ที่ได้รับมอบหมาย

๒.๔ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย ผู้ใช้งานควรปฏิบัติ ดังต่อไปนี้

๒.๔.๑ ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่มหาวิทยาลัย

๒.๔.๒ ไม่คัดลอกโปรแกรมต่างๆ ที่มหาวิทยาลัย ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๔.๓ ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

๒.๔.๔ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ

๒.๔.๕ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของมหาวิทยาลัย

เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย ได้เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ

๒.๔.๖ ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๓.๒ ผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานกว่า 30 นาที

๓.๓ มีการกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้ งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัยโดยการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) โดยจะทำการเก็บข้อมูลการทางจราจรคอมพิวเตอร์ (Log) ในกรณีนี้มหาวิทยาลัย ได้ใช้ระบบ Active Directory เป็นตัวควบคุม

๔. แนวปฏิบัติการใช้งานบัญชีผู้ใช้งาน (Account)

๔.๑ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๒ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๔.๓ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้ บัญชีผู้ใช้งาน (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕. ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและผ่านการฝึกอบรม หลักสูตร การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต มีรายละเอียด ดังนี้

๕.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสมตัวอย่าง เช่น จัดอบรม พรบ.คอมพิวเตอร์โดยผู้เชี่ยวชาญเฉพาะด้าน

๕.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) จัดให้มีการควบคุม และจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๕.๓ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) จัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ตัวอย่างเช่น เมื่อมีเจ้าหน้าที่หรือพนักงานของมหาวิทยาลัยลาออกจากงานไปแล้วโดยปกติ จะต้องทำการเก็บข้อมูลไว้

ระยะหนึ่งตามความเหมาะสมและความเห็นของผู้มีอำนาจตามสายงานนั้นๆ ซึ่งเมื่อถึงระยะรอบเวลาดังกล่าว สำนักวิทยบริการฯจะทำการสอบถามไปยังผู้มีอำนาจตามสายงาน โดยวิธีต่างๆอย่างเช่น จดหมายอิเล็กทรอนิกส์ (e-mail) หรือ บันทึกข้อความ ทั้งนี้ขึ้นอยู่กับความเหมาะสม ของแต่ละครั้งไป

๖. แนวปฏิบัติการใช้รหัสผ่าน (Password)

๖.๑ รหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆด้วย ควรใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น

๖.๒ ไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์ กับตนหรือคำศัพท์ที่ใช้ ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ และไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”“aaaaaa” หรือ “123456” เป็นต้น

๖.๓ ทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้ งานเครื่องคอมพิวเตอร์ของมหาวิทยาลัยทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๖.๔ ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

๖.๕ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

๖.๖ ผู้ใช้งานเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๖.๗ หากมีการนำอุปกรณ์สื่อสารสารสนเทศอื่นๆเข้ามาต่อพวงอย่างเช่น แฟลชไดร์ฟ, สมาร์ทโฟน, กล้องดิจิตอล ผู้ใช้งานจะต้องแน่ใจว่าอุปกรณ์เหล่านั้นไม่ก่อให้เกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์ภายในมหาวิทยาลัย

๗. แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

๗.๑ ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ เป็นลายลักษณ์อักษรแล้ว

๗.๒ ผู้ใช้งานต้องเข้าถึงระบบเทคโนโลยีสารสนเทศตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเท่านั้น และเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย ต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมเช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

๗.๓ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัย ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๗.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๗.๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย

๗.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น ใช้ข้อความที่ยั่วยุ ให้ร้าย อันจะก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยหรือการทำลายความสัมพันธ์กับบุคลากรของมหาวิทยาลัย

๗.๗ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานควรทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๘. แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑ แนวปฏิบัติการใช้งานสำหรับผู้ใช้งาน

๘.๑.๑ สำนักวิทยบริการฯ มีบริการจดหมายอิเล็กทรอนิกส์ โดยจะดำเนินการสร้างชื่อผู้ใช้งานพร้อมรหัสผ่านให้กับผู้บริหาร คณาจารย์ พนักงานหรือลูกจ้างในมหาวิทยาลัย โดยเป็นความลับเฉพาะเพื่อใช้งานจดหมายอิเล็กทรอนิกส์

๘.๑.๒ ผู้ใช้งานที่ได้รับรหัสผ่าน (Password) ครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันที

๘.๑.๓ ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๘.๑.๔ ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือนหรือตามระยะเวลาที่เหมาะสม

๘.๑.๕ ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ เว้นแต่จะได้รับความยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

๘.๑.๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้ใช้ งานควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้ามาสวมสิทธิ์การใช้งาน

๘.๑.๗ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑.๘ ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๘.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

๘.๒.๑ ผู้ดูแลระบบได้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (email) ของมหาวิทยาลัย ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย โดยจะต้องได้รับหนังสือจากต้นสังกัดของผู้ใช้งานเพื่อยืนยันการเพิ่มลดสิทธิ์รวมไปถึงการทำลายข้อมูล เป็นต้น

๘.๒.๒ ผู้ดูแลระบบได้กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๕ ครั้งหรือขึ้นอยู่กับความเหมาะสมกับระบบนั้นๆ

๙. แนวปฏิบัติให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยมีรายละเอียด ดังนี้

๙.๑ มีการจำกัดการเข้าถึงสารสนเทศ (Information access restriction) หรือควบคุมการเข้าถึงการใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่นตามความเหมาะสมหรือตามหน้าที่ที่ได้รับมอบหมาย

๙.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร จะได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ อย่างเช่น ระบบบริหารทรัพยากรบุคคล เป็นต้น

๙.๓ การควบคุมคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ได้กำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารตามความเหมาะสม

๙.๔ การควบคุมการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking) หรือ การควบคุมระยะไกล (Remote Desktop) กำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานภายนอกมหาวิทยาลัย ทั้งนี้มหาวิทยาลัยจะให้บริการในส่วนนี้ผ่านทางหน้าเว็บไซต์ซึ่งจะมีระบบไฟร์วอลล์ (Firewall) เป็นตัวควบคุมและบริหารจัดการการส่ง-รับข้อมูลผ่านการทำงานประเภทการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking) หรือการควบคุมระยะไกล (Remote Desktop)

ส่วนที่ ๓
แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายของมหาวิทยาลัย และป้องกันการบุกรุกผ่านระบบเครือข่าย หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของมหาวิทยาลัยได้อย่างถูกต้อง

๒. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

๒.๑ สำนักวิทยบริการฯ ได้กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย เพื่อดูแลรักษาความปลอดภัย โดยบุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้ งานระบบสารสนเทศของมหาวิทยาลัย จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักวิทยบริการฯ

๒.๒ ผู้ดูแลระบบ (System Administrator) ได้กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ ๑ ครั้ง

๒.๓ ผู้ดูแลระบบ (System Administrator) ได้จัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของมหาวิทยาลัย และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๒.๔ ผู้ดูแลระบบ (System Administrator) ได้จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๓. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ

สำนักวิทยบริการฯ ผู้ดูแลระบบ (System Administrator) ได้กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยให้สิทธิ์ เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งได้มีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๑ ผู้ดูแลระบบได้บริหารจัดการสิทธิ์ของผู้ใช้งาน ดังต่อไปนี้

๓.๑.๑ กำหนดจำแนกประเภทสิทธิ์ตามหน้าที่และความรับผิดชอบ โดยจัดเก็บและมอบหมายสิทธิ์ให้แก่ผู้ใช้งานระบบสารสนเทศซึ่งจะมีสิทธิ์ตามลำดับชั้นการเข้าถึงข้อมูล ดังนี้

๓.๑.๑.๑ ผู้บริหารระดับสูง (อธิการบดี, รองอธิการบดี, ผู้ช่วยอธิการบดี)

๓.๑.๑.๒ ผู้บริหารระดับกลาง (คณะบดี, ผู้อำนวยการ, รองคณบดี, รองผู้อำนวยการ)

๓.๑.๑.๓ ระดับวิชาการ (คณาจารย์, นักวิชาการ, นักวิจัย)

๓.๑.๑.๔ ระดับปฏิบัติการ (เจ้าหน้าที่ทั่วไป)

๓.๑.๑.๕ ลูกจ้าง (ลูกจ้างเหมาบริการ, พนักงานช่วยอำนวยการ)

๓.๑.๑.๖ ผู้ดูแลระบบ ในที่นี้หมายถึง เจ้าหน้าที่สำนักวิทยบริการฯมหาวิทยาลัย

๓.๑.๒ ในกรณีผู้ใช้งานมีความจำเป็นต้องใช้สิทธิ์สูงกว่าปกติ ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงข้อมูลระดับใดได้บ้าง โดยกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติเพื่อผู้ดูแลระบบจะได้ดำเนินการปรับค่าหรือแก้ไขต่อไป

๓.๑.๓ ทำการยกเลิกรหัสผ่าน (Password) เมื่อได้รับการแจ้งจากส่วนบริหารงานบุคคลหรือผู้อำนวยการฝ่าย เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่งหรือยกเลิกอำนาจหน้าที่

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔.๑ ผู้ดูแลระบบ (System Administrator) ดำเนินการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access- Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๔.๒ ผู้ดูแลระบบ (System Administrator) ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๔.๓ ผู้ดูแลระบบ (System Administrator) ดำเนินการกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง WirelessLAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สายตามความเหมาะสมในกรณีต่างๆ

๔.๔ ผู้ดูแลระบบ (System Administrator) ใช้วิธีการควบคุมผ่านระบบ AD (Active Directory) โดยกำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) สำหรับบุคลากรในมหาวิทยาลัย และใช้วิธีการควบคุมผ่านระบบ Firewall Authentication โดยกำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) สำหรับบุคคลภายนอก

๔.๕ ผู้ดูแลระบบ (System Administrator) ติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่าย ไร้สายกับระบบเครือข่ายภายในมหาวิทยาลัย

๔.๖ ผู้ดูแลระบบ (System Administrator) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้อำนวยการสำนักวิทยบริการฯ ทราบทันที

๔.๗ ผู้ดูแลระบบ (System Administrator) ควบคุมดูแลไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของมหาวิทยาลัย

๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๕.๑ สำนักวิทยบริการฯได้กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ไม่ใช่เจ้าหน้าที่สำนักวิทยบริการฯ โดยต้องลงทะเบียนขออนุญาต ระบุ วัน-เวลา เข้าออก และเหตุผลความจำเป็น

๕.๒ ผู้ใช้งานภายนอกที่จะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ และระบบเครือข่ายของมหาวิทยาลัย ต้องได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการฯและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๕.๓ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักโดยไม่ได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ

๕.๔ ผู้ดูแลระบบ (System Administrator) ควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๕.๔.๑ ใช้วิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๔.๒ มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๕.๔.๓ มีการกำหนดให้จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๕.๔.๔ ระบบเครือข่ายทั้งหมดของมหาวิทยาลัย ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกมหาวิทยาลัย ได้ถูกเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก และมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware)

๕.๔.๕ การเข้าสู่ระบบเครือข่ายภายในมหาวิทยาลัย ผ่านทางระบบอินเทอร์เน็ตได้กำหนดให้ลงบันทึกเข้า (Login) โดยระบุชื่อผู้ใช้งานและรหัสผ่านผู้ใช้ งานผ่านระบบพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

๕.๔.๖ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ที่สามารถระบุบนระบบเครือข่ายและอุปกรณ์บนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอและการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) มีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๕.๔.๗ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย จะต้องได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๔.๘ มีการป้องกันพอร์ตที่ใช้ สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ควบคุมการเข้าถึงพอร์ตที่ใช้ สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕.๔.๙ มีการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

๕.๔.๑๐ มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๕.๕ ผู้ดูแลระบบ (System Administrator) ทำหน้าที่บริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๕.๖ สำนักวิทยบริการฯได้กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังต่อไปนี้

๕.๖.๑ ความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ ในการจัดเก็บ กำหนดชั้นความลับในการเข้าถึงข้อมูลซึ่งผู้ดูแลระบบไม่ได้รับอนุญาตให้แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (Internal IT Auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

๕.๖.๒ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๕.๖.๓ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๕.๖.๔ วิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๕.๗ กำหนดมาตรการควบคุมการใช้ งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๕.๗.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของมหาวิทยาลัย จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ

๕.๗.๒ ผู้ดูแลระบบได้ควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๕.๗.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ

๕.๗.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้ งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับผู้อำนวยการสำนักวิทยบริการฯ

๕.๗.๕ การเข้าใช้งานต้องผ่านระบบการพิสูจน์ตัวตนจากระบบของมหาวิทยาลัย

๖. แนวปฏิบัติการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

สำนักวิทยบริการฯได้กำหนดมาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของมหาวิทยาลัย ในขณะที่ไม่มีผู้ดูแล ดังต่อไปนี้

๖.๑ ผู้ใช้งานต้องออกจาก (Log out) ระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานๆ

๖.๒ ป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตน

๖.๓ สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

๖.๔ เมื่อผู้ใช้งานระบบสารสนเทศทิ้งไว้ โดยไม่ใช้งานเป็นเวลานาน ระบบจะยุติการใช้งานระบบภายในระยะเวลา 10 นาที หรือตามความเหมาะสมขึ้นอยู่กับระบบนั้นๆ

๗. แนวปฏิบัติการลงทะเบียนผู้ใช้งาน

ผู้ดูแลระบบ (System Administrator) จัดทำขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานในการเข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว ดังต่อไปนี้

๗.๑ ทำการลงทะเบียนผู้ใช้งาน สำหรับระบบสารสนเทศของมหาวิทยาลัย ตามเอกสารหรือจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ได้รับแจ้งเป็นลายลักษณ์อักษรจากต้นสังกัดนั้นๆ

๗.๒ ตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๗.๓ ตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามข้อกำหนดของต้นสังกัด

๗.๔ แสดงเอกสารเป็นบันทึกหรือจดหมายอิเล็กทรอนิกส์ (e-mail) แจ้งให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศ

๗.๕ กำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๗.๖ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชี ผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่รับอนุญาต

๘. แนวปฏิบัติการดูแลสินทรัพย์สารสนเทศ

๘.๑ ผู้ดูแลระบบ (System Administrator) ทำหน้าที่ควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) สื่อบันทึกข้อมูล คอมพิวเตอร์หรือเทปบันทึก Back up ข้อมูล ซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิจัดเก็บไว้ในที่ที่ปลอดภัยในเวลาที่ไม่มีผู้ดูแล และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๘.๒ ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศที่มีความสำคัญหรือเป็นความลับของมหาวิทยาลัย ไว้ในที่ปลอดภัยภายหลังจากใช้งานเสร็จ

๘.๓ ผู้ใช้งานต้องป้องกันไม่ให้บุคคลภายนอกใช้กล้องดิจิตอล เครื่องสำเนาเอกสาร และเครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต

๙. แนวปฏิบัติการแบ่งแยกระบบเครือข่าย

ผู้ดูแลระบบ (System Administrator) ดำเนินการแบ่งแยกระบบเครือข่าย เป็นกลุ่มของผู้ใช้บริการและกลุ่มของระบบสารสนเทศ เพื่อจำกัดสิทธิการใช้งาน และควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น โดยแบ่งออกเป็น ๓ โซน ดังต่อไปนี้

๙.๑ โซนเครื่องคอมพิวเตอร์แม่ข่าย เป็นโซนที่มีการจัดเตรียมอุปกรณ์ และระบบเพื่อป้องกันและรักษาความมั่นคงปลอดภัยในระดับสูง เช่น ระบบตรวจจับและป้องกันผู้บุกรุก ระบบสำรองไฟฟ้า ระบบสำรองข้อมูล

๙.๒ โซนผู้ใช้งานภายในเป็นโซนสำหรับบุคคลากรในมหาวิทยาลัยโดยมีการติดตั้งระบบ Antivirus และระบบ Firewall

๙.๓ โซนภายนอก สำหรับบุคคลภายนอกให้สามารถเข้าถึงและใช้งานสารสนเทศภายในหน่วยงานผ่านอุปกรณ์ระบบรักษาความปลอดภัย Firewall หรือ (Intrusion Prevention System/Intrusion Detection System)

ส่วนที่ ๔
แนวปฏิบัติของผู้ดูแลระบบ

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบ (System Administrator) ในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย (Network) ให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลผู้ใช้งานให้เป็นไปตามแนวนโยบาย

๒. แนวปฏิบัติของผู้ดูแลระบบ (System Administrator)

๒.๑ ผู้ดูแลระบบ (System Administrator) มีอำนาจหน้าที่ ดังต่อไปนี้

๒.๑.๒ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่มหาวิทยาลัย ให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

๒.๑.๒ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย(Server) และระบบเครือข่ายอยู่เสมอ

๒.๑.๓ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๒.๑.๔ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย(Server) และระบบเครือข่าย

๒.๑.๕ เมื่อหมดความจำเป็นในการใช้งาน ด้วยวิธี การตามมาตรฐาน DOD5220.22-M ผู้ดูแลระบบจะทำการลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ข่าย (Server) อย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของมหาวิทยาลัย บนเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑.๖ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอและปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๒.๑.๗ ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้ งานของผู้ใช้งานที่พ้นสภาพการเป็นผู้ใช้งาน

๒.๑.๘ ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้ งานให้มีการกำหนดรหัสผ่าน(Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password)

๒.๑.๙ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๐ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์ หรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๑ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๒ เมื่อผู้ดูแลระบบ (System Administrator) พ้นจากหน้าที่ จะต้องคืนสินทรัพย์ของมหาวิทยาลัย ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้อำนวยการสำนักวิทยบริการฯหรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสินทรัพย์

๒.๒ ผู้ดูแลระบบ (System Administrator) ทำหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ใช้ วิธีการที่มั่นคงปลอดภัยดังต่อไปนี้

๒.๒.๑ เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

๒.๒.๒ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้เว้นแต่ ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (Internal IT Auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

๒.๒.๓ ในการเก็บข้อมูลจราจรนั้น สามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๒.๒.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ดูแลระบบได้ตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ส่วนที่ ๕
แนวปฏิบัติการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมในกรณีเกิดเหตุฉุกเฉินหรือไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของมหาวิทยาลัย

๒. แนวปฏิบัติการสำรองข้อมูล

๒.๑ ทุกหน่วยงานที่ใช้ระบบสารสนเทศสำรองข้อมูลและซอฟต์แวร์เก็บไว้ บนอุปกรณ์สำรองข้อมูล เป็นรายวันรายสัปดาห์ รายเดือน รายปี โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของมหาวิทยาลัย จากจำเป็นมากไปหาน้อย

๒.๒ ทุกหน่วยงานที่ใช้ระบบสารสนเทศจัดทำขั้นตอนการปฏิบัติการและจัดทำการสำรองข้อมูลและการกู้คืนข้อมูลอย่างสม่ำเสมอทุกเดือนหรือตามความเหมาะสมไปยังศูนย์กู้คืนระบบจากความเสียหายทางภัยพิบัติ (DR-Site) ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๒.๓ ทุกหน่วยงานที่ใช้ระบบสารสนเทศได้จัดเก็บอุปกรณ์ที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้ อย่างชัดเจนและทำการจัดเก็บเทปสำรองข้อมูลรายเดือนแยกไว้ ณ สถานที่อื่น

๒.๔ สำนักวิทยบริการฯได้เตรียมศูนย์คอมพิวเตอร์สำรอง (DR site) เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบงานตามลำดับความสำคัญคืนมาให้ใช้งานได้ภายในระยะเวลาที่เหมาะสม โดยมีการทดสอบปีละ ๒ ครั้ง

๒.๕ มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เป็นลำดับชั้น โดยผู้อำนวยการสำนักวิทยบริการฯเป็นผู้กำกับดูแลการปฏิบัติงาน

ส่วนที่ ๖
แนวปฏิบัติการประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

๒.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของมหาวิทยาลัย เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

๒.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๒.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๒.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๒.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

๒.๑.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต

๒.๑.๖ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒.๒ กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๒.๓ การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

๒.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๒.๓.๔ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๒.๓.๔ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในมหาวิทยาลัย เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ ความเสียหายหรืออันตรายที่จะเกิดขึ้นของหน่วยงาน

ส่วนที่ ๗
แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของมหาวิทยาลัย

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๘
การกำหนดผู้รับผิดชอบ

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. ระดับนโยบาย

ให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานที่ทำหน้าที่ CIO และผู้อำนวยการสำนักวิทยบริการฯ เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย ติดตามและกำกับดูแล ควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๒. แนวทางปฏิบัติของผู้รับผิดชอบ

๒.๑ ผู้อำนวยการสำนักวิทยบริการฯ รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

๒.๑.๑ ควบคุมการเข้า- ออกห้อง Server ตามการกำหนดสิทธิการเข้าถึง Server

๒.๑.๒ กำกับดูแล ตรวจสอบบำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๒.๑.๓ กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN , Internet , Intranet ที่ให้บริการในมหาวิทยาลัย

๒.๑.๔ กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของเครื่อง Server ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

๒.๑.๕ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๒.๑.๖ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ

๒.๑.๗ กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

๒.๑.๘ กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาตตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัย

๒.๑.๙ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์ ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๒.๒.๑๐ กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบอื่น ๆ

ประวัติผู้เขียน

1. ชื่อภาษาไทย นายวงเวียน วงค์กะโซ่
   ชื่อภาษาอังกฤษ Wongvian Wongkaso
2. ตำแหน่งปัจจุบัน นักวิชาการคอมพิวเตอร์ปฏิบัติการ
3. หน่วยงานและสถานที่อยู่ที่ติดต่อได้สะดวก
   680 หมู่ที่ – ถนนนิตโย ตำบลธาตุเชิงชุม อำเภอเมือง จังหวัดสกลนคร หมายเลขไปรษณีย์ 47000 หมายเลขโทรศัพท์ 0635163990 อีเมล์ wongvian@snru.ac.th
4. ประวัติการศึกษา
   ปริญญา ปริญญาตรี วุฒิ วทบ.เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสกลนคร

5.ประวัติการทำงาน

- นักวิชาการคอมพิวเตอร์ ลูกจ้างชั่วคราวรายเดือน สังกัดศูนย์คอมพิวเตอร์ สำนักวิทยาบริการ มหาวิทยาลัยราชภัฏสกลนคร (2550-2551) ลาออกเพื่อรับราชการทหารกองประจำการ
- นักวิชาการคอมพิวเตอร์ปฏิบัติการ สังกัดงานบริการการศึกษาและสารสนเทศ สำนักส่งเสริมวิชาการและงานทะเบียน มหาวิทยาลัยราชภัฏสกลนคร(2554-ปัจจุบัน)

6. ความเชี่ยวชาญ/ตำแหน่งงานที่ปฏิบัติ

- ใช้ชุดคำสั่ง SQL เพื่อจัดการข้อมูล
- พัฒนาระบบด้วยภาษา PHP ,C#
- ใช้โปรแกรม SPSS เพื่อวิเคราะห์ข้อมูล
- ดูแลและบริหารจัดการเครื่องแม่ข่ายคอมพิวเตอร์ ในรูปแบบเดิม และแบบใหม่ ด้วย Docker

7. ผลงานทางวิชาการ (ไม่เกิน 5 ปี ย้อนหลัง)